

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174797

(43)Date of publication of application : 23.06.2000

(51)Int.Cl. H04L 12/46  
 H04L 12/28  
 G11B 20/10  
 H04L 9/32  
 H04L 12/66  
 H04L 29/06

(21)Application number : 11-209836

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 23.07.1999

(72)Inventor : SAITO TAKESHI  
 TAKAHATA YOSHIAKI

(30)Priority

Priority number : 10292824

Priority date : 30.09.1998

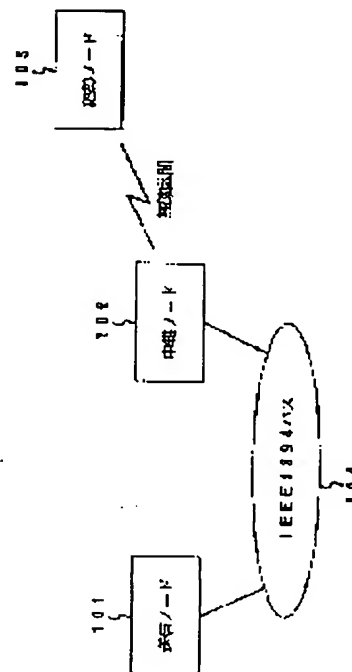
Priority country : JP

## (54) REPEATER AND COMMUNICATION EQUIPMENT

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a repeater capable of a contents protection procedure between equipment not connected to the same network.

SOLUTION: This repeater is connected to a first network 104 and a second network and is provided with a function for presenting the equipment 103 on the second network to the side of the first network 104 as the one on the present repeater 102, the function for transmitting a corresponding control command to the equipment 103 in the case of receiving the control command addressed to the equipment 103 from the equipment 101 on the first network 104, the function for transmitting contents protection information to the equipment 103 without changing it in the case of receiving it addressed to the equipment 103 from the equipment 101 and the function for transmitting contents to the equipment 103 without changing them in the case of receiving the contents protected by a contents key obtained from the previous contents protection information from the equipment 101 to the equipment 103.



## LEGAL STATUS

[Date of request for examination]

03.12.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3583657

[Date of registration] 06.08.2004

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-174797  
(P2000-174797A)

(43) 公開日 平成12年6月23日 (2000.6.23)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C
12/28		C 1 1 B 20/10	H
G 1 1 B 20/10		H 0 4 L 9/00	6 7 3 A
H 0 4 L 9/32			6 7 5 D
12/66		11/20	B
審査請求 未請求 請求項の数17 O L (全 60 頁) 最終頁に続く			

(21) 出願番号 特願平11-209836

(22) 出願日 平成11年7月23日 (1999.7.23)

(31) 優先権主張番号 特願平10-292824

(32) 優先日 平成10年9月30日 (1998.9.30)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 斉藤 健

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 高島 由彰

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 100058479

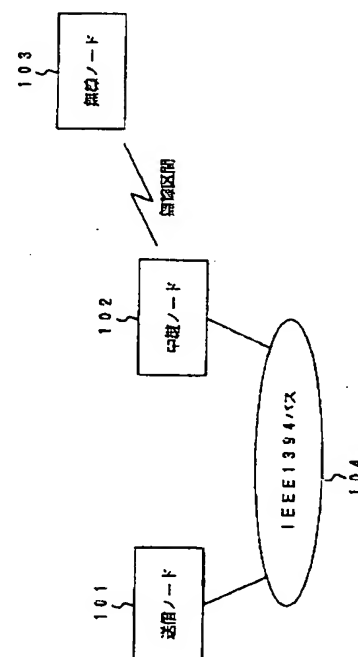
弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 中継装置及び通信装置

(57) 【要約】

【課題】 同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。

【解決手段】 第1のネットワーク104と第2のネットワークに接続され、第2のネットワーク上の装置103を自中継装置102上のもので第1のネットワーク104側に開示する機能と、第1のネットワーク104上の装置101から装置103宛の制御コマンドを受信した場合、これに対応する制御コマンドを装置103へ送信する機能と、装置101から装置103宛のコンテンツ保護情報を受信した場合、これに変更を加えずに装置103へ送信する機能と、装置101から装置103宛に先のコンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信した場合、これに変更を加えずに装置103へ送信する機能とを有する。



【特許請求の範囲】

【請求項1】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

前記第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第1のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第1のネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第2のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第1のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第2のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする中継装置。

【請求項2】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、

前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られる

コンテンツ鍵で保護されたコンテンツを受信するコンテンツ受信手段と、

このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする中継装置。

【請求項3】前記コンテンツ保護情報は、前記第1のネットワーク上の装置又はサービス又はサブユニットと、前記第2のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であることを特徴とする請求項2に記載の中継装置。

【請求項4】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第1のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第1のコンテンツ保護手段と、

前記第2のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第2のコンテンツ保護手段と、

前記第1又は第2のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第1又は第2のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第1又は第2のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項5】前記第1のコンテンツ保護手段と、前記第2のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであることを特徴とする請求項4に記載の中継装置。

【請求項6】前記コンテンツ受信手段と、前記コンテン

ツ送信手段は同一のLSIに封止されていることを特徴とする請求項4に記載の中継装置。

【請求項7】前記第1のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第2の鍵情報とを同一のものとすることを特徴とする請求項4に記載の中継装置。

【請求項8】前記第1又は第2のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうことを特徴とする請求項7に記載の中継装置。

【請求項9】前記第1及び第2のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマットの有無を含む構成情報を受信する構成情報受信手段と、

前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備したことを特徴とする請求項2または4に記載の中継装置。

【請求項10】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

前記第1のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第1のコンテンツ保護手段と、

前記第2のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第2のコンテンツ保護手段と、

前記第1又は第2のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第1又は第2のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第1又は第2のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、

前記第1のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第2の鍵情報とを同一のものとすることを特徴とする中継装置。

【請求項11】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行

なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、

前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、

この問合せに回答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする通信装置。

【請求項12】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、

前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、

前記ネットワーク上の他の装置から、前記問合せに該当するサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする通信装置。

【請求項13】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、

前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、

前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする通信装置。

【請求項14】前記所定のコンテンツ保護手続きに含ま

れる少なくとも一部の手續きにおいてやり取りされる情報に前記フローの識別子を付与することを特徴とする請求項21に記載の通信装置。

【請求項15】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手續きおよびまたは鍵交換手續きを含む所定のコンテンツ保護手續きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、

前記所定のコンテンツ保護手續きに含まれる少なくとも一部の手續きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする通信装置。

【請求項16】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

第1のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手續きおよびまたは鍵交換手續きを含む所定のコンテンツ保護手續きを行う第1のコピープロテクション処理手段と、

第2のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手續きおよびまたは鍵交換手續きを含む所定のコンテンツ保護手續き第2のコピープロテクション処理手段と、

前記第1のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第1のインタフェース手段から受信された前記暗号化されたデータを、前記第1のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第2のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第2のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項17】前記第2のネットワーク上の装置または

サービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示するとともに、前記第1のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第2のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、

前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示するとともに、前記第2のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第1のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、

前記代理構成手段は、前記第1または第2の一方のネットワーク上の装置と、前記第1または第2の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手續きおよびまたは鍵交換手續きを含む所定のコンテンツ保護手續きを行う場合には、前記第1または第2の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手續きを行うとともに、前記第1または第2の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手續きを行うことを特徴とする請求項24に記載の中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、IEEE1394バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及びIEEE1394バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【0002】

【従来の技術】近年、デジタル放送の開始や、デジタルAV機器の発売等、いわゆる「家庭AV環境のデジタル化」が大きな注目を集めている。デジタルAVデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【0003】しかしながら、このデジタルAV技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」の問題が発生する。

【0004】この「不正コピー」を防ぐための技術がい

くつか検討されている。その中の一つが、CPTWG（コピープロテクション技術ワーキンググループ）で検討されている「1394CPコンテンツ保護システム仕様（1394CP Content Protection System Specification）」である。この技術は、IEEE1394バスに接続されたノード間で、転送するコンテンツ（例えばMPEGデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【0005】

【発明が解決しようとする課題】IEEE1394バスは、最低速度でも100Mbps、網そのものに自動構成認識機能が備わっている、QOS転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルAV向けのネットワークとして、デファクトスタンダードの地位を築いている。

【0006】しかし、IEEE1394は、これら特徴のゆえに、「IEEE1394と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とIEEE1394バスを接続する場合は、これらの網が100Mbps以上といった高速性を一般には有していないことや、IEEE1394の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれないことから、IEEE1394プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、IEEE1394と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等が提案されている。

【0007】これらの方法を、従来の技術で述べた1394コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術がIEEE1394バスについてのみ定められている状況である。このコピープロテクション技術を「IEEE1394と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【0008】本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をIEEE1394の

みならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【0009】また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明（請求項1）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、前記第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のもので前記第1のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第1のネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第2のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第1のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第2のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする。

【0011】本発明（請求項2）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のもので各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、前記第1又は第2のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られるコンテンツ鍵で保護

されたコンテンツを受信するコンテンツ受信手段と、このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする。

【0012】好ましくは、前記コンテンツ保護情報は、前記第1のネットワーク上の装置又はサービス又はサブユニットと、前記第2のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であるようにしてもよい。

【0013】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第2のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニットを装置等と呼ぶ）」と「第1のネットワーク上の装置」の間において、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えずに中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第2のネットワーク上の装置等」と「第1のネットワーク上の装置」との間において行うことができる。

【0014】また、本発明によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、コンテンツを保護された形でエンドエンドに送り届けることができる。

【0015】本発明（請求項4）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第1のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第1のコンテンツ保護手段と、前記第2のネットワーク

上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第2のコンテンツ保護手段と、前記第1又は第2のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第1又は第2のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第1又は第2のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする。

【0016】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第2のネットワーク上の装置等」と「第1のネットワーク上の装置」の間において、「第1のネットワーク上の装置」または「第2のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第1のネットワーク上の装置」または「第2のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、例えば、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第2のネットワーク上の装置等」と中継装置との間、および中継装置と「第1のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【0017】また、第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【0018】好ましくは、前記第1のコンテンツ保護手段と、前記第2のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであるようにしてもよい。

【0019】好ましくは、前記コンテンツ受信手段と、前記コンテンツ送信手段は同一のLSIに封止されているようにしてもよい。これによって、この復号化手段と暗号化手段との間には、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【0020】好ましくは、前記第1のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第2の鍵情報とを同一のものとするようにしてもよい。これによって、一方のネットワークから伝えられた、他方のネットワーク



へ転送された暗号化データの鍵に関する情報（鍵やシード等）を、他方のネットワークへそのまま転送することにより、他方のネットワーク上の装置では該暗号化鍵の再生が可能となるため、コンテンツ受信手段とコンテンツ送信手段との間の暗号復号機能および再暗号化機能が不要となり、中継装置の大幅なコストの低減と、処理速度の高速化を図ることが可能となる。

【0021】また、好ましくは、他方のネットワーク側の装置と、暗号化されたデータの転送を行っている場合には、他方のネットワーク上の他の装置からの、暗号化が必要なデータの送信要求は拒否するようにしてもよい。このようにすれば、他方のネットワーク側において、異なる暗号化されたデータ転送を未然に防止することが可能となる。

【0022】好ましくは、前記第1又は第2のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうようにしてもよい。これによって、他方のネットワーク側の装置との間で、複数の暗号鍵を定義できるようになるため、暗号化されたデータを同時に転送することが可能となり、一方のネットワーク上の装置から複数の暗号化データが転送される場合あるいは一方のネットワーク上に複数の装置がある場合等への対処が可能となる。

【0023】好ましくは、前記第1及び第2のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマット（機器証明）の有無を含む構成情報を受信する構成情報受信手段と、前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備するようにしてもよい。これによって、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【0024】また、好ましくは、前記代理構成手段は、前記第1のネットワークの装置に対してデータを送信する際に、あらかじめ該第1のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。これによって、この通知を受信した第1のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【0025】本発明（請求項10）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、前記第1のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第1のコンテンツ保護手段と、前記第2のネットワーク上の装置又はサービス又は

サブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第2のコンテンツ保護手段と、前記第1又は第2のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第1又は第2のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第1又は第2のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、前記第1のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第2の鍵情報とを同一のものとすることを特徴とする。

【0026】本発明（請求項11）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、この問合せに回答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする。

【0027】本発明（請求項12）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、前記ネットワーク上の他の装置から、前記問合せに該当す

るサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする。

【0028】本発明によれば、特定の仮想チャネルで転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、特定の識別子を持って転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【0029】本発明（請求項13）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする。

【0030】好ましくは、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与するようにしてもよい。

【0031】本発明によれば、フロー毎に異なる鍵の定義ができるようになるため、以降の認証・鍵交換で、「このフローに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【0032】本発明（請求項15）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与さ

れた暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする。

【0033】本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは仮想チャネルから送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグから、あるいは前記特定の識別子を持って、送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【0034】本発明（請求項16）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う第1のコピープロテクション処理手段と、第2のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第2のコピープロテクション処理手段と、前記第1のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第1のインタフェース手段から受信された前記暗号化されたデータを、前記第1のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第2のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第2のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【0035】本発明によれば、第1のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第1のネットワークと第2のネットワークの通信帯域が著しく異なる場合のように、第2のネットワークに元のデータとは異なるデータ形式で転送することが求め

られた場合に、変換手段によってデータ形式の変換を行いつつ、第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【0036】好ましくは、請求項16に記載の中継装置において、前記第2のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示するとともに、前記第1のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第2のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示するとともに、前記第2のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第1のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、前記代理構成手段は、前記第1または第2の一方のネットワーク上の装置と、前記第1または第2の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第1または第2の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第1または第2の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うようにしてもよい。

【0037】本発明によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間で、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【0038】また、好ましくは、請求項16に記載の中継装置において、前記コンテンツ受信手段は、前記第2のコピープロテクション処理手段を用いて、前記第2のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第1のコピープロテクション処理手段を用いて、前記第1のネットワーク上の装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。このようにすれば、第2のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第2のネットワーク上の装置等と認証手続きを行い、その後、第1のネットワーク上の装置等との認証に失敗した場合に、第1のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

【0039】また、本発明に係る通信装置は、第1の装置の制御に供される画面描画のためのプログラムを含む、第1の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第1の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、前記パネル画面をサブユニットとして第2の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第1の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよい。ため、簡単な計算環境を用意しておけばよい。本発明によれば、前記制御プログラムを持たない第2の装置に対しても、パネル画面という形で、前記第1の装置の制御インタフェースを提供することが可能になる。

【0040】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0041】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0042】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0043】(第1の実施形態)図1は、ある家庭のホームネットワークの全体構成の一例である。

【0044】このホームネットワークには、送信ノード101、中継ノード102、無線ノード103の3つが接続されており、送信ノード101と中継ノード102は(有線の)IEEE1394バス104に、中継ノード102と無線ノード103は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

【0045】本実施形態では、送信ノード101から送出されたMPEG映像を、中継ノード102で中継し、無線区間を経由して無線ノード103に送信する場合を例として説明する。その際に、著作権保護(不正コピーの防止)のために、送信ノード101と無線ノード103との間で転送されるMPEG映像データは暗号化される場合を考える。

【0046】なお、図1では、3つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい(後述する他の実施形態においても同様である)。

【0047】図2に、送信ノード101の内部構造の一例を示す。

【0048】送信ノード101は、内部にMPEG映像データを蓄積している装置であり、要求に応じてMPEG映像データをIEEE1394バス104を通じて送出する。その際、IEEE1394バス上において不法コピーをされることを未然に防止するために、必要な場合には送出するMPEG映像データを暗号化して送出する機能を持つ。そのため、MPEG映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

【0049】図2に示されるように、この送信ノード101は、IEEE1394インタフェース401、AV/Cプロトコルの処理を行うAV/Cプロトコル処理部402、AV/Cプロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部403、IEEE1394を通して送受信されるデータのうち、同期チャンネルを通してやり取りされるデータについて送受信するISO信号送受信部404、MPEG映像のストレージであるMPEGストレージ部406、コピープロテクション処理部403から暗号鍵Kをもらい、MPEG映像を暗号化してISO信号送受信部404に送出する暗号化部405を有する。ここで、コピープロテクション処理部403は、認証のためのフォーマットAcertを持つ。

【0050】次に、図3に、中継ノード102の内部構造の一例を示す。

【0051】中継ノード102は、IEEE1394バ

ス側から受信したデータ(MPEG映像データ)を無線区間側にフォワードする機能の他に、IEEE1394バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してIEEE1394バス側のノード(本実施形態では送信ノード101)の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能が存在する。

【0052】図3に示されるように、この中継ノード102は、IEEE1394インタフェース201、無線インタフェース202、AV/Cプロトコル処理部203、ISO信号送受信部204、無線区間側の同期チャンネルの信号の送受信を行う無線ISO信号送受信部205、IEEE1394バス上のノードの構成情報を収集したり、自らの構成情報(自分がどのような機能を持っているかについての情報等)をIEEE1394上に広告する機能を持つ1394バス構成認識部206、IEEE1394バス側に対して無線区間側のノードやサービス(サブユニット)を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してIEEE1394側のノード/サービス(サブユニット)の代理公開やコマンドの代理受付/翻訳等を行う代理サブユニット構成部207、無線区間上のノードの構成情報を収集したり、自らの構成情報(自分がどのような機能を持っているかについての情報等)を無線区間上に広告する機能を持つ無線区間構成認識部209、コピープロテクションに関する処理を行い、1394バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御/フォワード部210、無線区間でやり取りされる制御バケットの送受信を行う無線ノード制御バケット送受信部211を有する。

【0053】次に、図4に、無線ノード103の内部構造の一例を示す。

【0054】無線区間においていわゆるIEEE1394プロトコル(物理レイヤプロトコル、リンクレイヤプロトコル等)が稼働している必要は必ずしもなく、IEEE802.11や無線LAN等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆるQOS機能(同期通信機能)を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分にQOS機能が求められると制限されるものではない。

【0055】いわゆるIEEE1394ノードではない無線ノード103が、IEEE1394バスにつながれたノード(本実施形態では送信ノード101)と通信を行うために、前述のように、中継ノード102がIEEE1394バス上のノードや機能(サブユニット)をエ

ミュレートしている。すなわち、無線ノード103から見て、中継ノード102はいわゆるIEEE1394バス側のノードや機能の代理サーバとなっている。無線ノード103は、これら（IEEE1394側のノードや機能）を中継ノード102の機能と考え、通信を行うが、実際には中継ノード102が必要なプロトコル変換やデータの乗せ換えを行う。

【0056】図4に示されるように、この無線ノード103は、無線インタフェース301、無線ノード制御パケット送受信部302、コピープロテクション処理部303、無線ISO信号送受信部304、受信した暗号化されたストリーム（MPEG映像等）を、コピープロテクション処理部303から渡されるコンテンツキーKを使ってこれを復号化する暗号復号化部305、MPEGデコード部306、映像を表示するディスプレイ部307を有する。

【0057】無線ノード103のコピープロテクション処理部303は、後述するように、認証フォーマットBcertを持ち、その認証の発行機関は、送信ノード101（の映像送出サブユニット）の認証フォーマットAcertの発行機関と同一の発行機関である。

【0058】次に、実際のコピープロテクションを施した上でのMPEG映像全体のシーケンスについて、図5／図6（全体のシーケンス例）、図7／図8（送信ノード101のフローチャート例）、図9／図10／図11（中継ノード102のフローチャート例）、図12／図13（無線ノード103のフローチャート例）を参照しながら説明する。

【0059】まず、無線ノード103は、自分の構成情報を中継ノード102に通知する（ステップS501）。この通知は、無線ノード内にIEEE1212レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つといったことや、認証・鍵交換のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、IEEE1394向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

【0060】ここで、認証について簡単に説明する。

【0061】ネットワーク上で映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能になってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

【0062】次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たと

え、データを暗号化して送ったとしても、送った先のノード（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

【0063】具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上で転送する、という手法をとる。

【0064】さて、無線ノード103は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード103が持っている認証フォーマットを「Bcert」とする。

【0065】無線ノード103は、図5のステップS501で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップS801）。例えば、図14のように、構成情報の中に、本無線ノード103がMPEGデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

【0066】なお、中継ノード102が無線ノード103の構成を認識する方法としては、この他にも中継ノード102が無線ノード103に対して構成を問い合わせるパケットを送信し、無線ノード103がこれに答える方法等も可能である。

【0067】さて、この構成情報を受信した中継ノード102は、無線ノード103が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS701）。

【0068】中継ノード102は、無線ノード103がMPEGデコード／ディスプレイ機能を持っていることをIEEE1394バス側のノードに対して知らせるため、このMPEGデコード／ディスプレイ機能を、中継

ノード102自身のサブユニットとしてIEEE1394バス側に広告する(ステップS502)。具体的には、IEEE1212レジスタに「自分はMPEGデコード/ディスプレイ機能を持っている」旨を記載したり、AV/Cプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がMPEGデコード/ディスプレイサブユニットを持っているという形で応答を返したりする(これにより、IEEE1394に接続されたノードは、中継ノード102にこの機能が存在すると認識することになる)。

【0069】そのために、中継ノード102は、代理サブユニット構成部207内に代理テーブル208を持つ。代理テーブル208は、図15/図16のように、中継ノード102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0070】ここでは、図15のように、無線ノード103のMPEGデコード/ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される(ステップS702, S703)。

【0071】このため、送信ノード101から見た中継ノード102の構造は図17のように見えることになる(ステップS601)。

【0072】以上は、IEEE1394バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図16のような設定がなされ、無線ノードから見た中継ノード102の構造は図18のように見える。

【0073】さて、中継ノード102内にMPEGデコード/ディスプレイサブユニットがあると認識した送信ノード101は、このサブユニットに対して、MPEG映像を転送することを目的に、1394バス上に同期チャンネル#xを確立し、AV/Cプロトコルにて「この同期チャンネル#x(を受信するプラグ(例えば1394TAにて規定されたAV/Cにおけるプラグ))と、MPEGデコード/ディスプレイサブユニットとを接続し、映像を表示せよ」との命令をだす(ステップS503, S602)。送信ノード101は、このサブユニットが中継ノード101にあたるものと解釈しているため、命令の送信先は中継ノード102である。

【0074】これを受信(ステップS704)した中継ノード102は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているMPEGデコード/ディスプレイサブユニットに対する命令であることを認識し、代理テーブル208を参照して、この命令先の実体は無線ノード103にあることを認識する(ステップS705)。

【0075】よって、IEEE1394バスの同期チャ

ネル#xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャンネル(#y)の確保を行い(ステップS706)、さらにISO信号送受信部204(同期チャンネル#xを受信)と無線ISO信号送受信部205(同期チャンネル#yを送信)を接続し、1394インタフェース201から入力された入力データ(ISOデータ)を無線区間にフォワードできるようにする(ステップS504, S707)。

【0076】さらに、無線ノード103に対して、「無線同期チャンネル#yを通してデータを送信するので、これを受信し、MPEGデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する(ステップS505, S708)。

【0077】図19に、この無線ノード制御パケットの一例を示す。

【0078】図19に示されるように、無線ノード103に無線同期チャンネル#yを通して送信したデータ(MPEG映像)を、MPEGデコード/ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ(MPEG映像)を送信するサブユニット(中継ノード102の映像送信機能; 実際には、送信ノード101の代理でその機能を持っていると広告している)についての情報も併せて通知している。

【0079】これを受信した無線ノード103は、無線同期チャンネル#yを通してデータが送られてくることを認識する(ステップS802)。無線ノード103は、このデータの送信元は中継ノード102の映像送信サブユニットであると認識する(前述のように、実際のデータ送信元は送信ノード101である)。このため、この無線ノード制御パケット内に、「この無線同期チャンネルを通して送信されるデータの送信元は中継ノード102の映像送信サブユニットである」との情報を含めてもよい。

【0080】この後、送信ノード101は、同期チャンネル#xを通して、暗号化されたMPEG映像を転送する(ステップS603, S506)。これを受信した中継ノード102は、先に設定したようにこれを無線区間にフォワードする(ステップS709, S507)。

【0081】中継ノード102は、ステップS506で暗号化されたMPEG映像を受信した時点で、これが暗号化データであることを認識できるが、無線網側に転送する必要があると認識し、これをそのままフォワードする。後に認証・鍵交換の手続きが必要である旨を記憶しておいてもよい。

【0082】このようにして、暗号化されたMPEG映像が無線ノード103に到達する(ステップS803)。このMPEG映像には、ソースアドレスとして中継ノード102のノードIDが含まれていてもよい。このため、無線ノード103は、このMPEG映像が中継



ノード102から到達したものであることまでは認識できるが、この時点で無線ノード103はこの暗号を解くための鍵Kを有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、この状態で暗号を解いて、MPEG映像を取り出すことはできない。ここで、無線ノード103は認証手続きがMPEG映像の送信元と必要であることを認識する。

【0083】そこで、無線ノード103（のコピープロテクション処理部303）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード103には、上記暗号化データの送信元は中継ノード102（内の、サブユニット種別=映像送信サブユニット、かつ、サブユニットID=b（b=0とする）の、サブユニット）であるように認識されている。

【0084】また、図5のS521のように、中継ノード102に対して、「無線ノードにおいて、無線同期チャンネル#yを受信しているのは、サブユニット種別=MPEGデコード/ディスプレイサブユニットで、かつ、サブユニットID=c（c=0とする）の、サブユニットである。無線同期チャンネル#yに暗号化データを送信しているのはどのサブユニットか？」という意味合いの問い合わせを送信してもよい。これに対し、中継ノード102は、「無線同期チャンネル#yに送信しているのは、映像送信サブユニットのサブユニットID=0である。」との返答を返す（ステップS522、S731、S831）。これにより、無線ノード103は、認証を行なう先が中継ノードの映像送信サブユニットであることを認識できる。

【0085】このように、認証要求の宛先を認識し、中継ノード102（内の映像送信サブユニットのサブユニットID=0）に対し、認証要求を送信する。この送信の仕方として、認証要求パケットの宛先を「中継ノードの映像送信サブユニット（のサブユニットID=0）」としてもよいし、認証要求パケットの任意の位置に「映像送信サブユニット（のサブユニットID=0）」という情報を入れ、認証要求先は映像送信サブユニット（のサブユニットID=0）であると言うことを明確に表示してもよい。前者の場合は、中継ノードの各サブユニット内に認証・鍵交換の手続きが含まれていることを意味する。後者の場合は、中継ノードのある特定の処理部が、一括して、各サブユニットの認証・鍵交換を行なうことを意味する。

【0086】その際、認証要求には、無線ノード103の認証フォーマットBcertを付与する（ステップS804、S508）。Bcertは、無線ノード103のMPEGデコード/ディスプレイサブユニットの認証フォーマットであってもよい。なお、コピープロテクション処理部は、サブユニット毎（サブユニット種別毎）でなく、サブユニットID毎に認証フォーマットを用意してもよい。

【0087】認証要求を受信（ステップS710）した中継ノードは、代理テーブル208を参照して、この認証要求の要求先が実は送信ノード101（の映像送信サブユニットのサブユニットID=a（a=0とする））であることを認識する。

【0088】中継ノード102は、送信ノード101に対して、「中継ノードにおいて、同期チャンネル#xを受信しているのはMPEGデコード/ディスプレイサブユニットのサブユニットID=0である。同期チャンネル#xに暗号化データを送信しているのは、送信ノードのどのサブユニットか？」という意味合いの問い合わせを送信してもよい（ステップS523、S631、S732）。これに対し、送信ノード101は、「同期チャンネル#xに送信しているのは、映像送信サブユニットのサブユニットID=0である。」との返答を返す（ステップS524、S631、S732）。

【0089】このようにして、認証要求の相手を認識したならば、ステップS508にて受信した認証要求を、中身を変えずに（Bcert等はそのまま残して）送信ノード101に対してフォワードする（ステップS509、S711）。すなわち、宛先アドレスや、認証要求の宛先であるサブユニット以外の認証フォーマット等は、中継ノードは透過的に転送できる。

【0090】認証要求の転送の際は、先に説明したように、認証要求パケットの宛先を映像送信サブユニット（のサブユニットID=0）としてもよいし、認証要求パケットの任意の位置に当該サブユニットを明示する情報を入れ、認証要求先は当該サブユニットであると言うことを明確に表示してもよい。

【0091】ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード101に到達することになり、結局、送信ノード101と無線ノード103との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード102をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【0092】認証要求を受け取った送信ノード101は、これを中継ノード102のMPEGデコード/ディスプレイサブユニットから送られてきた認証要求であると解釈する（ステップS604）。その後、Bcertから無線ノード103のMPEGデコード/ディスプレイサブユニットを特定できるID（Bdid）を抽出し（ステップS605）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード101は、Bcertが無線ノード103の認証フォーマットであるとは意識することはなく、むしろ中継ノード102（のMPEGデコード/ディスプレイサブユニット）の認証フォーマットであると意識をしている。

【0093】この認証要求には、送信ノード101（の映像送出サブユニット）の認証フォーマットAcertと、Bdidとが含まれる。ここで、送信ノード101は、該認証要求（ステップS509）の送信元は中継ノード102（のMPEGデコード／ディスプレイサブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード102となる（ステップS606、S510）。

【0094】これを受信（ステップS712）した中継ノード102は、代理テーブル208を参照して、この認証手続の本来の要求先が無線ノード103（のMPEGデコード／ディスプレイ機能）であることを認識し、この認証手続要求を、中身を変えずに（Acert等はそのまま残して）無線ノード103に対してフォワードする（ステップS511、S713）。この認証要求の送信元は中継ノード102である。

【0095】これを受け取った無線ノード103は、これを中継ノード102の映像送信サブユニットから送られてきた認証要求であると解釈する（ステップS805）。その後、Acertから送信ノード101の映像サブユニットを特定できるID（Adid）を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード103は、Acertが送信ノード101の認証フォーマットであるとは意識せず、むしろ中継ノード102（の映像送信サブユニット）の認証フォーマットであると意識する。

【0096】この認証鍵の交換に必要な残りの手続きとして、無線ノード103は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップS512）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、Acertの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスID（Adid）等が含まれている（ステップS806）。ここで、無線ノード103は、該認証要求（ステップS511）の送信元は中継ノード102（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード102となる。

【0097】これを受信した中継ノード102は、代理テーブル208を参照して、この認証手続きの本来の要求先が送信ノード101（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード101に対してフォワードする（ステップS513、S714）。このパケットの送信元は中継ノード102である。

【0098】これと同様の手続きが送信ノード101→中継ノード102→無線ノード103の方向に対しても行われる（ステップS514、S515、S609、S715、S807）。

【0099】この認証手続きパケットを受信した送信ノード101および無線ノード103は、それぞれ、受信したパケットが改ざんされていないかどうかのタンバの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Kauthを導き出す。この共通の認証鍵Kauthは、送信ノード（の映像送信サブユニット）と無線ノード（のMPEGデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵Kauthを、この両者（送信ノード101、無線ノード103）以外の他人に知られることなく共有することがこの時点で行えるようになる（ステップS607、ステップS608、S808）。

【0100】この認証鍵Kauthを使って、実際にMPEGストリームの暗号化を行うコンテンツキーKの計算ができるようになる。具体的な手順はここでは省略するが、送信ノード101から無線ノード102に、IEE1394のコピープロテクション方式（5C方式）のように、交換鍵やシード（種）の値を別途送ることにより、コンテンツキーKの計算ができるようになっていてもよい（ステップS518、S519）。

【0101】さて、このようにして、送信ノード101（の映像送信サブユニット）と無線ノード103（のMPEGデコード／ディスプレイ機能）との間で、コンテンツキーKの値が共有できるようになった。

【0102】ここで、送信ノード101が、送信するMPEG映像を、コンテンツキーKを使って、暗号化部405にて暗号化し（ステップS610）、これを1394バスの同期チャンネル#xを通して中継ノード102（のMPEGデコード／ディスプレイサブユニット）に対して送信する（ステップS516、S611）。

【0103】中継ノード102は、送信ノード101から同期チャンネル#xを通して送られてくる暗号化されたMPEG映像を、ISO信号送受信部204から無線ISO信号送受信部205を通して、無線同期チャンネル#yに送信する（ステップS517、S716）。

【0104】これを受信した無線ノード103は、キーKの値を使ってMPEG映像の値を復号化する（ステップS809、ステップS810）。復号化されたMPEGデータは、MPEGデコード部306にて復号化され（ステップS811）、これをディスプレイ部307にて再生表示する（ステップS812）。

【0105】このように、1394バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード101と無線ノード103）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継ノード102を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のMPEG映像等のコンテンツ保護に必要なデータの転送も、コピーが不可能



のように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0106】なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第2の実施形態で説明するので、例えばこれを適用すればよい。

【0107】また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【0108】(第2の実施形態)次に、第2の実施形態について説明する。

【0109】第1の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード(の映像サブユニット)と無線ノード(のMPEGデコード/ディスプレイ機能)とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのMPEGデコード/ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【0110】これに対し、第2の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、1394バス区間のMPEGデータの暗号化転送についての責任を終端するとともに、無線区間のMPEGデータの暗号化転送についての責任を終端する場合の例である。

【0111】図20に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第1の実施形態と同様である。

【0112】図21に、送信ノード2101の内部構造の一例を示す。これも第1の実施形態と基本的には同様である。

【0113】次に、図22に、中継ノード2102の内

部構造の一例を示す。

【0114】中継ノード2102は、第1の実施形態と同様に、IEEE1394バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してIEEE1394バス側のノード(本実施形態では送信ノード2101)の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能を持つ。

【0115】また、IEEE1394バス側から受信したデータ(MPEG映像データ)を無線区間側にフォワードする機能を持つが、第1の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがIEEE1394バス区間と無線区間との両方について、この中継ノード2102において終端されており、IEEE1394バス側については認証フォーマットBcertをIEEE1394コピープロテクション処理部2208に、無線区間側については認証フォーマットCcertを無線区間コピープロテクション処理部2212にそれぞれ持ち、1394バスの同期チャネルから入力されてきた暗号化データについては、ISO信号受信部2203にて受信→暗号復号化部2204にて暗号復号化→復号化されたMPEG映像を、暗号化部2205にて再暗号化→無線ISO信号送受信部2206にて、無線同期信号上に送信、というプロセスを踏む点である。

【0116】これらの認証フォーマットは、IEEE1394インタフェース毎、あるいは無線区間インタフェース毎に1つずつもっていてもよいし、(代理も含めて)サブユニット毎(サブユニット種別毎)に1つずつ持っていてよい。

【0117】ここで、AcertとBcertは、同じ認証機関(例えばIEEE1394のコピープロテクションを担当する認証機関)が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット(後述するCcertとDcert)については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【0118】次に、図23に、無線ノード2103の内部構造の一例を示す。コピープロテクション処理部2303が、無線区間向けの認証フォーマットDcertを持っていること以外は、基本的には第1の実施形態の無線ノードと同様である。

【0119】次に、実際のコピープロテクションを施した上でのMPEG映像全体のシーケンスについて、図24/図25(全体のシーケンス例)、図26/図27(送信ノード2101のフローチャート例)、図28/図29/図30/図31(中継ノード2102のフローチャート例)、図32/図33(無線ノード2103のフローチャート例)を参照しながら説明する。

【0120】まず、無線ノード2103は、自分の構成情報を中継ノード2102に通知する（ステップS2501）。構成情報とは、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つことといったことや、認証のための認証フォーマットを持っていることなどである（図14参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップS2801）。

【0121】これを受信した中継ノード2102は、無線ノード2101が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS2701）。中継ノード2102は、第1の実施形態と同様に、このMPEGデコード／ディスプレイ機能を、IEEE1212レジスタやAV／Cプロトコル等を使って、中継ノード2102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS2502）。

【0122】そのために、中継ノード2102は、代理サブユニット構成部2210内に代理テーブル2214を持つ。この代理テーブル2214は、基本的には第1の実施形態と同様であり、図34／図35のように、中継ノード2102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0123】ここでは、図34のように、無線ノード2103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS2702、S2703）。

【0124】このため、送信ノード2101から見た中継ノード2102の構造は、図36のように見えることになる（ステップS2601）。

【0125】以上は、IEEE1394バス側についての説明であったが、第1の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード2102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理服务無線区間側に行っている。よって、図35のような設定がなされ、無線ノードから見た中継ノード2102の構造は図37のように見える。

【0126】さて、中継ノード2102内にMPEGデコード／ディスプレイサブユニットがあると認識した送信ノード2101は、このサブユニットに対して、MPEG映像を転送することを目的に、1394バス上に同期チャンネル#xを確立し、AV／Cプロトコルにて「この同期チャンネル#x（を受信するプラグ）と、MPEGデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップS2503、S2602）。送信ノード2101は、このサブユニットが中継ノード2102にあるものと解釈しているため、命令の送信先は中継ノード2102である。

【0127】これを受信（ステップS2704）した中

継ノード2102は、受信した命令パケットを解釈し、その命令が自らが代理服务を行っているMPEGデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル2210を参照して、この命令先の実体は無線ノード2103にあることを認識する（ステップS2705）。

【0128】ここで、図20の無線区間は、QOS対応の無線LANになっており、予め定められた手順を踏めば、パケット廃棄や遅延等の品質劣化無く、転送データを送信先まで転送することが可能であるとする。この無線LAN上では、データは図38のように、イーサネットフレームと同様のフォーマット、すなわち「送信元アドレス、宛先アドレス、データ」のようなフォーマットを持つ、無線フレームで転送される。

【0129】さて、IEEE1394バスの同期チャンネル#xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間のQOS設定を行う。さらにISO信号送受信部2203（同期チャンネル#xを受信）と無線ISO信号送受信部2206（QOS保証を行なう無線フレームにて送信）を図22の点線のように接続し（まだ暗号の復号化ができないため）、1394インタフェース2201から入力されたISO入力データを無線区間にそのままフォワードできるようにしてもよい（ステップS2504、S2706、S2707）。

【0130】さらに、無線ノード2103に対して、「上記無線フレームを通して、データを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を無線ノード制御パケットの形で送信する（ステップS2505、S2708、S2802）。この制御プロトコルには、IEEE1394AV／Cプロトコル、あるいはIEC61883プロトコルや、これらを変形したものを用いてもよい。後述するように、本実施形態では、無線LAN上に同期チャンネルの概念はないものの、転送するデータにソースID（SID）なる領域を設け、無線区間にQOSデータを送信しているノード毎に、転送しているQOSデータを一意に区別できるようになっており、このSIDの値をIEEE1394の同期チャンネルのように、データフローの判別に用いることができる。無線ノード制御パケットの一例を図39に示す。パケットの送信元は中継ノード2102である。

【0131】これを受信した無線ノード2103は、 $\alpha$ なるSIDが付与されて、データがQOS転送されてくることを認識する。

【0132】この後、送信ノード2101は、同期チャンネル#xを通して、暗号化されたMPEG映像を転送する（ステップS2506、S2603）。コンテンツ鍵はK1とする。この暗号鍵は、後述する交換鍵やシードの関数として導出される。

【0133】また、この暗号化されたMPEG映像を送信するフレームには、同期チャンネル番号の他、送信ノー

ドを識別する「送信ノードID」が含まれていてもよい。

【0134】これを受信した中継ノード2102は、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードID」を参照して、このデータを送信しているのが送信ノード2101であることを認識し（ステップS2709）、送信ノード2101に対して、「同期チャンネル#xを通して、このデータを送出しているのは、送信ノード2101のどのサブユニットか」を確かめるため、認証先の問合せを行なう（ステップS2507、S2710）。この際、データが転送されている同期チャンネル番号（#x）を記載して、送信ノード2101が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する自身のサブユニット（本実施形態の場合、中継ノード2102のMPEGデコード/ディスプレイサブユニットのサブユニットID=0）も通知する。これは、送信ノード2101から見た認証先を通知する役割を持つ。

【0135】なお、この認証先問合せパケットと、後述する認証先応答パケットは、認証機関のプライベート鍵でハッシュや暗号化したデータを電子署名として記載しておき、改ざん等が無いことを確認できるようにしてもよい。

【0136】さて、認証先問合せを受信（ステップS2604）した送信ノード2101は、同期チャンネル#xに対して送信しているデータを受信しているサブユニットが、中継ノード2102のMPEGデコード/ディスプレイサブユニットであることを認識するとともに、自らが該同期チャンネル#xに送信しているサブユニットが、映像送信サブユニット（サブユニットID=0）であることを、認証先応答パケットとして、中継ノード2102に通知する（ステップS2508、S2605）。

【0137】これにより、中継ノード2102は、同期チャンネル#xにデータを送信しているサブユニットが、送信ノード2101の映像送信サブユニット（サブユニットID=0）であることを認識できる（ステップS2711）。

【0138】同期チャンネル#xにデータを送信しているサブユニットが、送信ノード2101の映像送信サブユニットであることを認識した中継ノード2102（のMPEGデコード/ディスプレイサブユニットの代理機能）は、続いて送信ノード2101の映像送信サブユニットに対して認証要求を行なう。この認証要求には、中継ノード、あるいは中継ノードのMPEGデコード/ディスプレイサブユニットの認証フォーマット（Beret）が共に転送される（ステップS2509、S2606、S2607、S2712）。この認証要求と認証フォーマットの交換は、第1の実施形態と同様に、送信ノ

ード2101（の映像送信サブユニット）から中継ノード2102（のMPEGデコード/ディスプレイサブユニット）に向けても行われる（ステップS2510、S2608、S2713、S2714）。このように、第2の実施形態においても、認証・鍵交換にサブユニットに関する情報も交換するのは、同じ装置同士の通信でも、通信しているサブユニットが異なれば、異なる鍵の使用ができるようにするためである。

【0139】お互いに認証が完了した両ノードは、第1の実施形態と同様に認証・鍵交換手続きを行い（ステップS2511、S2512、S2609、S2715）、認証鍵Auth1を共有する。この認証鍵を使って、送信ノード2101は、交換鍵やシードの転送を中継ノード2102に対して行ない（ステップS2512、S2610、S2716）、結局、中継ノード2102では、コンテンツ鍵K1の値を知ることができるようになる（ステップS2717）。

【0140】以降、転送されてくるコンテンツ鍵K1で暗号化されたMPEG映像（同期チャンネル#x経由）（ステップS2513、S2611、S2612）は、中継ノード2102にて復号化され（ステップS2514、S2718）、さらに無線区間用に別に用意されたコンテンツ鍵k2で再暗号化され（ステップS2515、S2516、S2719）、無線区間上をQOSが保証される形で、無線ノード2103に対して送信される（ステップS2517、S2720、S2803）。この時点では、MPEG映像はISO信号送受信部2203、暗号復号化部2204、暗号化部2205、無線ISO信号送受信部2206というパスを通る。

【0141】先に述べたように、このとき中継ノード2102が、無線区間側に送信しているデータの区別ができるようにするために、ソースIDなる、中継ノード2102で一意な値を付与して送出してもよい。ここでは、この一意な値を $\alpha$ とする。すなわち、 $\alpha$ の値のついたデータは、IEEE1394の同期チャンネル#xから受信したデータ（をコンテンツ鍵K1で復号化し、コンテンツ鍵K2で再暗号化したもの）である。中継ノード2102は、 $\alpha$ のSIDを付けて無線区間に送出しているデータは、自身の無線区間側の映像送信サブユニットの代理機能から送信しているデータであることを認識している。

【0142】これを受信した無線ノード2103の動作は、基本的に先に説明した、暗号化データを受信した中継ノード2102の動作と同様である。すなわち、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信元アドレス」を参照して、このデータを送信しているのが中継ノード2102であることを認識し、中継ノード2102に対して、「 $\alpha$ なる値を付与して、このデータを送出しているのは、中継ノード2102のどのサブユニットか」を確かめるた

め、中継ノードに認証先の問合せを行なう（ステップS2518、S2804）。

【0143】この際、データが転送されているSIDの値（ $\alpha$ ）を記載して、中継ノード2102が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する受信側のサブユニット（本実施形態の場合、無線ノード2103のMPEGデコード／ディスプレイサブユニットのサブユニットID＝0）も通知する。これは、中継ノード2102から見た認証先を通知する役割を持つ。

【0144】認証先問合せを受信（ステップS2721）した中継ノード2102は、SID＝ $\alpha$ に対して送信しているデータを受信しているサブユニットが、無線ノード2103のMPEGデコード／ディスプレイサブユニット（サブユニットID＝0）であることを認識するとともに、自らがSID＝ $\alpha$ を付与して送信しているサブユニットが、映像送信サブユニットであることを、認証先応答パケットとして、無線ノード2103に通知する（ステップS2519、S2722、S2805）。

【0145】これにより、無線ノード2103は、SID＝ $\alpha$ を付与してデータを送信しているサブユニットが、中継ノード2102の映像送信サブユニットであることを認識できる。

【0146】SID＝ $\alpha$ を付与してデータを送信しているサブユニットが、中継ノード2102の映像送信サブユニットであることを認識した無線ノード2103（のMPEGデコード／ディスプレイサブユニット）は、続いて中継ノード2102の映像送信サブユニットに対して認証要求を行なう（ステップS2520、S2723、S2724、S2806）。この認証要求には、無線ノード（または無線ノードのMPEGデコード／ディスプレイサブユニット）の認証フォーマット（Dcert）が共に転送される。この認証要求と認証フォーマットの交換は、中継ノード2102（の映像送信サブユニット）から無線ノード2103（のMPEGデコード／ディスプレイサブユニット）に向けても行われる（ステップS2521、S2725、S2807）。

【0147】お互いに認証が完了した両ノードは、続いて認証・鍵交換手続きを行い（ステップS2522、S2523、S2726、S2808）、認証鍵Kauth2を共有する。この認証鍵を使って、中継ノード2102は、交換鍵やシードの転送を無線ノード2103に対して行い（ステップS2524、S2727、S2809）、結局、無線ノード2103で、コンテンツ鍵K2の値を知ることができるようになる（ステップS2810）。

【0148】なお、これまでの説明では送信ノードと中継ノード間の認証・鍵交換と、中継ノードと無線ノード間の認証・鍵交換とは、順次行われる形で説明したが、

逆の順番でもよいし、両者を並行して行うことも可能である。

【0149】以降、転送されてくるコンテンツ鍵K1で暗号化されたMPEG映像（ステップS2525）は、中継ノード2102にて復号化され（ステップS2526）、さらに無線区間用に別に用意されたコンテンツ鍵K2で再暗号化され（ステップS2527、S2528、S2728）、無線区間上をQOSが保証される形で、SID＝ $\alpha$ が付与された無線フレームの形で無線ノード2103に対して送信される（ステップS2529、S2729）。

【0150】今度は、無線ノード2103は、先に入手した交換鍵、シードの値を使って、コンテンツ鍵K2を計算できるので、これを復号化することが可能であり（ステップS2530、S2811）、これをディスプレイ部2307にて再生する（ステップS2812）。

【0151】このように、IEEE1394バスと無線網の間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送が可能になる。

【0152】もちろん、中継ノード2102の「生のMPEGデータ」が流れる部分、具体的には暗号復号化部2204と暗号化部2205との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のLSIにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）することが実質的に不可能になるため、このような対策を行っておくことが有益である。

【0153】（第3の実施形態）次に、第3の実施形態について説明する。

【0154】第3の実施形態では、IEEE1394上において、HAVi規格（Specification of the Home Audio/Video Interoperability（HAVi）Architecture）等に代表される、AV/Cの上位レイヤに相当するAV機器制御ソフトウェアが稼働している場合における実施形態である。

【0155】図40に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第1の実施形態と同様である。

【0156】図41に、送信ノード4101の内部構造の一例を示す。これも第1の実施形態の場合とほぼ同様

であるが、IEEE1212レジスタ4407を強調のため、追加記述している。IEEE1212レジスタ4407には、送信ノード4101の属性、例えば「どのベンダの製品かを示す情報、例えばVTRやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置URL、制御アイコン、コマンド一覧」等の情報が含まれる。

【0157】次に、図42に、中継ノード4102の内部構造の一例を示す。中継ノード4102も、第1の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なIEEE1212レジスタ4213を1394バス構成認識部4206内に特に記した点と、HAVi処理部4212を持つ点が第1の実施形態と異なる。HAVi処理部4212には、いわゆるHAViバイトコードの処理を行う仮想マシン（VM）が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成部4207が持つ。

【0158】次に、図43に、無線ノード4103の内部構造の一例を示す。これについても、第1の実施形態の場合と基本的には同様である。

【0159】次に、HAVi環境における、実際のコピープロテクションを施した上でのMPEG映像全体のシーケンスについて、図44／図45（全体のシーケンス例）、図46／図47（送信ノード4101のフローチャート例）、図48／図49／図50（中継ノード4102のフローチャート例）、図51／図52（無線ノード4103のフローチャート例）を参照しながら説明する。

【0160】まず、無線ノード4103は、自分の構成情報を中継ノード4102に通知する（ステップS4501）。このとき、これらの構成情報は、IEEE1212レジスタ形式の情報として中継ノード4101に送付するものとする。すなわち、中継ノード4102が、無線ノード4103に対して「IEEE1212で規定されるCSR（コマンド・ステータスレジスタ）空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード4103が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード4103が持っている認証フォーマットをBcertとする。

【0161】これを受信した中継ノード4102は、無線ノード4101が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS4701）。中継ノード4102は、無線ノード4101がMPEGデコード／ディスプレイ機能を持っていることをIEEE1394バス側の

ノードに対して知らせるため、このMPEGデコード／ディスプレイ機能を、中継ノード4102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS4502）。具体的には、自身のIEEE1212レジスタに「自分はMPEGデコード／ディスプレイ機能を持っている」旨を記載したり、AV／Cプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がMPEGデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード4101等のIEEE1394に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

【0162】そのために、中継ノード4102は、代理テーブル4208を持つ。代理テーブル4208は、図53／図54のように、中継ノード4102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0163】ここでは、図53のように、無線ノード4103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS4702、S4703）。

【0164】以上と逆の手続きがIEEE1394バス4104上の送信ノード4101の代理登録を無線区間側に対してみせる形で行われる（ステップS4503、S4504）。すなわち、送信ノード4101のIEEE1212レジスタ4407に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード4102が読み込む（ステップS4601、S4704）。この送信ノード4101の機能を、中継ノード4102の機能として、代理して無線区間側のIEEE1212相当機能（無線区間側のCSR空間）に反映し、無線ノード4103側には、上記映像送信機能、およびパネル機能が中継ノード4102の機能であるものとして認識してもらう。この対応関係を、代理テーブル4208に図54のように反映する（ステップS4705）。

【0165】このようにして代理テーブル4208は、図53／図54のように構成される。また、送信ノード4101から見た中継ノード4102の内部構造を図55に、無線ノード4103から見た中継ノード4102の内部構造を図56に、それぞれ示す。

【0166】なお、この時点で、ステップS4503の送信ノード構成情報の中に、送信ノード4101を制御するためのHAViのバイトコードが含まれており、中継ノード4102は送信ノード4101の代理サーバ、すなわちDCM（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード4102のHAVi処理部4212内の仮想マシン上で稼働することになる。

【0167】さて、中継ノード4102にパネル機能が

あるものと認識した無線ノード4103は、中継ノード4102の(パネルサブユニット)に対して、パネルの表示要求のコマンドを送出する(ステップS4505、S4802)。これを受信(ステップS4706)した中継ノード4102は、代理テーブル4208を参照し、このパネル機能の実体が送信ノード4101に存在していることを認識し、前記パネル表示要求コマンドを送信ノード4101に対してフォワードする(ステップS4506、S4707)。

【0168】これを受信(ステップS4601)した送信ノード4101は、AV/Cプロトコルにてパネル応答(つまり、制御画面の送信)を行う。送信先は、中継ノード4102である(ステップS4603、S4507)。これを受信(ステップS4708)した中継ノード4102は、代理テーブル4208を参照して、これを無線ノード4103にフォワードする(ステップS4709、S4508、S4803)。

【0169】ここで、図57に、無線ノード4103に送られてきた制御画面の一例を示す。この制御画面(パネル)では、6つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン1」、「ボタン2」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン1が押されました」というコマンドの形で、パネルの送信元に送られる仕組みとなっているものとする。

【0170】さて、無線ノード4103は、中継ノード4102が提供していると認識している映像送信サービスを受けようと考え(実際に提供しているのは送信ノード4101)、無線ノード制御パケットを使って(ステップS4509)、映像を流すための無線同期チャンネル#yを確保し、このチャンネルを中継ノード4102の映像送信サブユニットに接続するためのコマンドを中継ノード4102に対して発行する(ステップS4804)。これを受信した中継ノード4102は、代理テーブル4208を参照して、実際にこのAV/Cコマンドが発行されるべきノード(送信ノード4191)を確認し、IEEE1394バス上に必要な帯域を確保するとともに(同期チャンネル#x)、内部のISO信号送受信部4204を設定して、IEEE1394バスの同期チャンネル#xと無線同期チャンネル#yとを相互に接続する(ステップS4710、S4711、S4712、S4510)。また、中継ノード4102は、送信ノード4101に対し、同期チャンネル#xを映像送信サブユニットに接続するコマンドを発行する(ステップS4511、S4713)。これを受信(ステップS4604)した送信ノード4101は、映像送信サブユニットの実体である内部の映像ストリームの流れるパス(図41で2重矢印になっている部分)をIEEE1394バスの同期チャンネル#xに接続する。

【0171】これと前後して、無線ノード4103のユ

ーザは、見たい映像を選択するために図57のパネルの中から適当な番組を選択すべく、制御画面のボタンを押す(例えば、マウスを使ってクリックする、ペン入力する、タッチする、など)。この操作は、中継ノード4102に伝達され、これは代理テーブル4208の参照を経て送信ノード4101へのコマンドに変換される(ステップS4805、S4714、S4715、S4605、S4512、S4513)。

【0172】この後、送信ノード4101は、同期チャンネル#xを通して、暗号化されたMPEG映像を転送する(ステップS4514、S4606)。これは、中継ノード4102にて中継され、無線ノード4103に到達する(ステップS4716)。

【0173】後の手続きは、第1の実施形態の場合と同様であり、暗号化されたMPEG映像が無線ノード4103に到達する(ステップS4806)が、この時点で無線ノード4103はこの暗号を解くための鍵を有していないため、MPEG映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第1の実施形態と同様であるので、ここでの詳細な説明は省略する。

【0174】なお、第1の実施形態に従えば、認証は送信ノード4101の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能との間で行われると考えられるが、第3の実施形態の場合には、このような認証方式の他に、送信ノード4101のパネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード4101のパネルにデバイスIDが割り当てられることになる。

【0175】なお、HAViにおいては、送信ノード4101から送られてくるバイトコードであるDCM等の中に、送信ノード4101を制御するための制御画面情報が含まれる場合がある。このようなモジュールをDDI(データドリブンインタラクション)と呼ぶ。このようなモジュールは、例えば中継ノード4102内のHAVi処理部4212にて展開され、制御画面が生成される。本実施形態では、この制御画面(あるいは、それと同等の機能を持つ制御画面)を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部4207が、このDDIに含まれる画面構成情報を認識して(例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる)、パネルとしてこの制御画面を再構成し、無線区間に「パネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル4208には、このパネルと、DDIで生成されるべきHAViやAV/Cのコマンド(中継ノード4102から送信ノード4101に対して発行される)の対応テーブルが用意されることになる。この方法は、無線ノード4103内にHAViバイトコードの仮想マシンが存在



しなくても有効であるため、H A V i 仮想マシンを持たない無線ノード4103から、H A V i 機器の制御を可能とする方法である。

【0176】(第4の実施形態)次に、第4の実施形態について説明する。

【0177】図58に、本実施形態の全体構成の一例を示す。

【0178】図58に示されるように、第4の実施形態では、ある家庭のホームネットワークであるIEEE1394バス6104と、公衆網(ここでは、一例としてインターネットとするが、電話網等でもよい)6105とが、ホームゲートウェイ6102で接続され、送信ノード6101と受信ノード6103との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット6105(のアクセス網部分)は、IEEE1394バス6104と比べて通信帯域が非常に細く、IEEE1394バスでやり取りされる映像情報(一例としてMPEG2映像であるとする)は、帯域が足りずに通せないため、ホームゲートウェイ6102においてトランスコーディング、つまりMPEG2符号からMPEG4符号への符号変換を行った上で、伝送を行うことを考える。

【0179】第4の実施形態においても、第2の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイ受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が1394バス区間および無線区間のMPEGデータの暗号化転送についてのそれぞれの責任を終端する。

【0180】次に、図59に、送信ノード6101の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【0181】次に、図60に、ホームゲートウェイ6102の内部構造の一例を示す。

【0182】ホームゲートウェイ6102の基本的な構成は、無線インタフェースではなくインターネットインタフェース6202を有している点、代理サブユニット構成部ではなく代理ホームページ作成部6210を有している点、ホームページの作成・蓄積部6211を有している点、暗号復号化部6204と暗号化部6205との間にMPEG2/MPEG4変換部6214を有している点を除くと、第2の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【0183】ホームゲートウェイ6102は、インターネット側のノードに対してIEEE1394バス側のノード(本実施形態では、送信ノード2101)の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能を持つ。送信ノード6101が提供しているサービス(本実施形態の場合、映像送信サービス)には、ホームゲートウェイ6102が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード6103からは、送信ノード6101のサービスは、ホームゲートウェイ6102のホームページを介して見えるため、これをホームゲートウェイ6102が提供するIP(インターネット)上のサービスとして解釈されてもよい。

【0184】また、ホームゲートウェイ6102は、第2の実施形態と同様に、IEEE1394バス側から受信したデータ(MPEG2映像データ)をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクションに関する手続きがIEEE1394バス区間とインターネット区間との両方について、このホームゲートウェイ6102において終端されている。IEEE1394バス側については、認証フォーマットBcertをIEEE1394コピープロテクション処理部6208に、インターネット区間側については、認証フォーマットCcertをインターネット側コピープロテクション処理部6212にそれぞれ持ち、IEEE1394バスの同期チャネルから入力されてきた暗号化データについては、ISO信号送受信部6203にて受信→暗号復号化部6204にて暗号復号化→復号化されたMPEG2映像をMPEG2/MPEG4変換部6214にてトランスコード→MPEG4映像を暗号化部6205にて再暗号化→AV信号送受信部6206にてインターネット側に送信、というプロセスを踏む。

【0185】ここで、AcertとBcertは、同じ認証機関(例えばIEEE1394のコピープロテクションを担当する認証機関)が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット(後述するCcertとDcert)については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【0186】なお、本実施形態においては、認証フォーマット(Acert~Dcert)は、ノード(あるいはネットワークインタフェース)毎に1つ持つのではなく、サブユニット毎(サブユニット種別毎)、あるいはインターネットアプリケーション毎に1つ持つてもよい。すなわち、異なるインターネットアプリケーションでは、異なる認証フォーマットを用いてもよい。ここで、フローとは、インターネットの(送信アドレス、送信ポート、受信アドレス、受信ポート)の組で表現され

る一連のデータ流を指す。

【0187】次に、図61に、受信ノード6103の内部構造の一例を示す。

【0188】コピープロテクション処理部6303がインターネット向けの認証フォーマットDcertを持っている。第2の実施形態との相違点は、インタフェース（インターネットインタフェース6301、制御パケット送受信部6302、AV信号送受信部6304）がインターネット対応となっている点である。ここで、制御パケット送受信部6302はTCP、AV信号送受信部6304はUDPのトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

【0189】次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図62／図63（全体のシーケンス例）、図64／図65（送信ノード6103のフローチャート例）、図66／図67／図68／図69（ホームゲートウェイ6102のフローチャート例）、図70／図71（受信ノード6103のフローチャート例）を参照しながら説明する。

【0190】まず、ホームゲートウェイ6102は、送信ノード6101のIEEE1212レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する（ステップS6501、S6601、S6701、S6502、S6602、S6702）。これを通して、ホームゲートウェイ6102は、送信ノード6101が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【0191】これを受けて、ホームゲートウェイ6102は、送信ノード6101を遠隔制御するためのホームページを作成する（ステップS6503）。基本的には、送信ノード6101が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード6101のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部6210内の交換テーブルに対応の一覧が記述される。例えば、送信ノード6101のパネルサブユニットに「再生」とかかっているボタンが存在する場合には、該ホームページにも「再生」とかかっているボタンを用意して、この関係を前記交換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ6102から送信ノード6101のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図72（a）に送信ノード6101のパネルサブユニットの持つパネルの一例を、図72（b）にホームゲートウェイ6102の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【0192】さて、インターネット上の受信ノード6103は、インターネットを介してこのホームゲートウェイ

6102にアクセスし、送信ノード6101の制御画面を含むホームページを要求し、このホームページが送付される（ステップS6504、S6801、S6703）。これを見て、受信ノード6103のユーザは、画面上の映像送信を要求するボタン（例えば、図72

（b）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」というインタラクションが、インターネット経由でホームゲートウェイにHTTPを通じて通知される（ステップS6505、S6802、S6704）。

【0193】この通知と前後して、ホームゲートウェイ6102と受信ノード6103との間で、やり取りされるストリームが転送されるIPフロー、すなわち（送信IPアドレス、送信ポート、受信IPアドレス、受信ポート）の組の決定や、セッション制御（符号化方式や認証方式等）のネゴシエーション等が行なわれる（ステップS6505、S6705、S6803）。例えば、RTSP（リアルタイムトランスポートストリーミングプロトコル）やSDP（セッションデスクリプションプロトコル）等を用いて、符号化方式や認証の方式、ポートの番号の決定などが行われる。

【0194】ホームゲートウェイ6102は、これらの処理を受け、映像送信を行なう実体は、送信ノード6101の映像送信サブユニットであることを認識し、送信ノード6101に対してAV/Cプロトコル等で、データ転送のための同期チャンネル#xの設定や、映像送信サブユニットに対して、映像送信の要求などのコマンドを発行する（ステップS6506）。

【0195】これを受けて、送信ノード6101から同期チャンネル#xを通して、暗号化されたMPEG映像がホームゲートウェイ6102に対して送出される（ステップS6507、S6603、S6604）。その後は、第2の実施形態のIEEE1394側の手順と同様の手順で、認証先問合せ／応答、認証要求、認証・鍵交換手続き、交換鍵／シード転送等が行われ、ホームゲートウェイ6102にてコンテンツ鍵K1の計算ができるようになる（ステップS6508～S6514、S6605～S6611、S6706～S6715）。

【0196】以降、同期チャンネル#xを通して暗号化されたMPEG映像（ステップS6515、S6612、S6613）を受信したホームゲートウェイ6102は、暗号復号化部6204にて、これをコンテンツ鍵K1を用いてMPEG2映像に復号化する（ステップS6516、S6517、S6716）。次に、抽出したMPEG2映像を、MPEG2/MPEG4変換部6214でMPEG4映像にトランスコードする（ステップS6518）。このMPEG4映像を、コンテンツ鍵K2を用いて、暗号化部6205で再暗号化し（ステップS6519、S6520、S6717、S6718）、これをIPパケット化する。その場合、先のセッション制



御の手順で決めたように、送信IPアドレスはC（ホームゲートウェイのIPアドレス）、送信ポート番号はc、受信IPアドレスはD（受信ノードのIPアドレス）、受信ポート番号はdであるようなIPパケットを生成する（ステップS6521、S6719）。

【0197】これを受信した受信ノード6103は、受信したデータが暗号化されていることを認識する（ステップS6804）。受信ノード6103は、このデータを送信しているのは、到着したパケットのIPヘッダを参照すること等により、ホームゲートウェイ6102であることを認識し、ホームゲートウェイ6102に対して、認証要求を送信する（ステップS6522、S6805）。この認証要求のパケットもIPパケットでもよい。認証要求のためのポート番号は、認証を行なう手続きに予め割当てられている番号を用いてもよい。この際、この認証要求のパケットに、ストリーム転送のフローID（C、c、D、d）を付与して転送する。このことにより、ホームゲートウェイ6102は、どのフローに対する認証要求であるかを認識することができる。図示はしていないが、この認証要求には、受信ノードの（本ストリーム用の）認証フォーマット等も含まれている。

【0198】また、トランスポートプロトコルとしてRTP（Realtime Transport Protocol）を用いていること等を同時に伝えてもよい。

【0199】これを受けてホームゲートウェイ6102は、フロー（C、c、D、d）のための認証要求であることを認識し、このフローのための認証フォーマットを含んだ認証要求を、受信ノード宛てに送り返す（ステップS6523、S6720～S6722、S6806、S6807）。このとき、この認証要求には前記フローID等が含まれる。

【0200】次に、両者は、認証・鍵交換手続き、交換鍵／シードの転送等を、IPパケット上で行う（ステップS6524～S6526、S6723、S6724、S6808～S6810）。これにより、受信ノード6103は、コンテンツ鍵K2の生成が行なえるようになっている。

【0201】よって、以降、コンテンツ鍵K2にて暗号化された、フロー（C、c、D、d）を通して送られてくるMPEG4データ（ステップS6527～S6533、S6725、S6726、S6811）は、上記のように用意されたコンテンツ鍵k2にて復号化することが可能となる（ステップS6534）。復号化されたMPEG4データは、MPEGデコード部6306にて復号化され（ステップS6812）、これをディスプレイ部6307にて再生する（ステップS6813）。

【0202】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホー

ムゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0203】第2の実施形態と同様に、ホームゲートウェイ6102において、「生のMPEGデータ」が流れる部分、具体的には暗号復号化部6204、MPEG2/MPEG4変換部6214、暗号化部6205との間は、データコピーがなされないようにするための工夫、例えば一体のLSIに封止する等の対策を立てておいてもよい。

【0204】（第5の実施形態）次に、第5の実施形態について説明する。

【0205】第4の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第5の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【0206】図73に、本実施形態の全体構成図を示す。

【0207】図73に示されるように、第5の実施形態では、2つの家庭網8105、8107が公衆網（ここでは、一例としてインターネットとするが、B-ISDN等でもよい）8106にて接続されている。第1の家庭網8105上の送信ノード8101から、コピープロテクションを考慮した形で、AVコンテンツを第2の家庭網8107上の受信ノード8104に送信する。ここで、第4の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【0208】第5の実施形態においては、第1の実施形態の中継ノードと同様に、ホームゲートウェイ8102、8103にて、IEEE1394バス8105、8107上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ8102、8103は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【0209】送信ノード8101や受信ノード8104は、基本的には第4の実施形態と同様の構成である。

【0210】図74に、ホームゲートウェイ8102、8103の内部構造の一例を示す。

【0211】ホームゲートウェイ8102の基本的な構

成は、コピープロテクションを終端しない点（これは、第1の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第1の実施形態の中継ノードと同様）を除き、第4の実施形態のホームゲートウェイの構成とはほぼ同様である。

【0212】図75に、全体のシーケンスの一例を示す。

【0213】ここでは、第2の家庭網8107のユーザが、ホームゲートウェイ8103の制御画面を使って、送信ノード8101のコンテンツを、インターネット8106を介して受信ノード8104に配信させる場合を考える。

【0214】まず、第4の実施形態と同様に、ステップS8301の構成認識と、ステップS8302の送信ノード制御用ホームページ作成が行われる。

【0215】第2の家庭網8107のユーザは、ホームゲートウェイ8103を操作し、ホームゲートウェイ8102から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップS8303）。また、例えば図76に例示するような受信ノード8104の制御画面も同時に開く。そこで、図76のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ8103に映像配信を命令する（ステップS8304）。

【0216】すると、第4の実施形態と同様に、映像送信要求がホームゲートウェイ8102に（インターネットコマンドとして）発行され（ステップS8305）、これがホームゲートウェイ8102にてAV/Cプロトコルコマンドに翻訳され、送信ノード8101から受信ノード8104間の通信バス（IEEE1394バス8105上の同期チャンネル#x、インターネット上のコネクション、IEEE1394バス上の同期チャンネル#y）が設定される（ステップS8306、S8307）。この上を、暗号鍵Kで暗号化されたMPEG2映像が配信される（ステップS8308～S8310）。

【0217】第1の実施形態と同様に、これを受信した受信ノード8106は、送信元に認証要求を発行する（ステップS8311）。受信ノード8104は、この映像はホームゲートウェイ8103から配信されていると解釈しているため、この認証要求はホームゲートウェイ8103に対して行われる。

【0218】ホームゲートウェイ8103は、第4の実施形態と同様に、内部の変換テーブル8211を参照して、これをホームゲートウェイ8102にフォワードする。これは、ホームゲートウェイ8103は、映像の配信元がホームゲートウェイ8102であると解釈しているからである。このフォワードは、認証要求8311の中身を変えない形で、インターネットパケットで行われる（ステップS8312）。同様に、ホームゲートウェイ8102は、これを受信ノード8101にフォワード

する（ステップS8313）。送信ノード8101は、これをホームゲートウェイ8101から発行された認証要求であると解釈する。

【0219】これと同様の手順を双方向に組み、送信ノード8101と受信ノード8104間で認証手続きが行われる（ステップS8314）。この間、ホームゲートウェイは、この手続きのパケットの中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード8104は鍵の入手を行い、結局、暗号化されたMPEG2映像の復号化ができるようになる。

【0220】しかして、送信ノード8101が送信するMPEG映像を、コンテンツキーKを使って暗号化し、これが1394バスの同期チャンネル#x、ホームゲートウェイ8102、公衆網、ホームゲートウェイ8103、1394バスの同期チャンネル#yという経路を辿って、受信ノード8103に到達する（ステップS8315～S8317）。そして、受信ノード8103では、暗号化されたMPEG映像は、暗号鍵Kを使って暗号復号化され、デコードされて、再生表示される。

【0221】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0222】なお、第5の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第4の実施形態の符号化変換（例えば、ホームゲートウェイ8102ではMPEG2/MPEG4変換、ホームゲートウェイ8103ではMPEG4/MPEG2変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

【0223】（第6の実施形態）第1の実施形態においては、中継ノードがIEEE1394バスと無線網との両方に接続され、IEEE1394バス上の送信ノードと無線網上の無線ノードとの間で暗号化された映像データのやり取りをする場合の、認証・鍵交換方式を説明した。第1の実施形態では、認証フォーマットの交換等に代表される実際の認証・鍵交換は、送信ノードと無線ノード間で直接行ない、中継ノードは、これらのデータを透過的に中継する形で、これを実現してきた。

【0224】これに対し、第6の実施形態では、第2の実施形態のように、認証・鍵交換の単位を送信ノードと中継ノード間、および中継ノードと無線ノード間でそれぞれ行なう。ただし、第2の実施形態と異なり、中継ノ

ードにてコンテンツデータの暗号の復号化、および再暗号化を行なう必要が無いような方法の説明を行なう。すなわち、第2の実施形態では、到着したデータについて、中継ノードにてIEEE1394区間の暗号の復号化を行い、無線区間の暗号化を再度行なうといった手順を使っていたが、これに対し、第6の実施形態では、IEEE1394バス側から到着した暗号化データをそのまま無線網上に転送できるような方法である。

【0225】図77に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第2の実施形態と同様である。

【0226】図78に、送信ノード9101の内部構造の一例を示す。これも第2の実施形態と基本的には同様である。認証フォーマットAcertが、ノードに一つ用意されている。

【0227】図79に、中継ノード9102の内部構造の一例を示す。認証フォーマットBcert、Ccertが、ネットワークインタフェース毎に一つ（IEEE1394側にBcert、無線網側にCcert）用意されている。IEEE1394側のISO信号送受信部9203と無線ISO信号送受信部9206間で、（復号化／再暗号化のプロセスを経ずに）直接暗号化されたストリーム信号がやり取りされる点を除いて、第2の実施形態と同様である。

【0228】図80に、無線ノード9103の内部構造の一例を示す。これも第2の実施形態と基本的には同様である。認証フォーマットDcertが、ノードに一つ用意されている。

【0229】これまでの実施形態と同様に、中継ノードでは、IEEE1394側には無線網上のサービスの、無線網側にはIEEE1394上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【0230】次に、本実施形態の全体のシーケンス例を図81に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（MPEG映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でIEEE1394上は同期チャンネル#x上を、無線網上は無線同期チャンネル#y上を転送されるものとする。なお、詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【0231】また、送信ノード9101の動作手順例を図82に、中継ノード9102の動作手順例を図83／図84に、無線ノード9103の動作手順例を図85／図86に、それぞれ示す。

【0232】本実施形態では、IEEE1394上の著作権保護方式である「5C Digital Transmission Content Protection Specification」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。なお、本実施形態では、認証・鍵交換方式をノード単位で行う場合について説明する（サブユニット単位で行う場合については、第7の実施形態で説明する）。

【0233】さて、送信ノード9101は、IEEE1394の同期チャンネル#x上に、コンテンツ鍵Kで暗号化されたMPEG映像を転送する（ステップS8501、S8601、S8701）。これを受信した中継ノード9102は、このまま（受信したMPEG映像を、コンテンツ鍵Kで暗号化されたまま）無線網側の無線同期チャンネル#yに対して転送する（ステップS8509、S8701）。

【0234】同期チャンネル#yを通して受信したデータが暗号化されていると認識した中継ノード9102は、到着したデータのCIPヘッダの送信ノードIDフィールド（SIDフィールド）を参照する等して、送信ノード9101と認証・鍵交換すべきであると認識する（ステップS8801）。中継ノード9102の認証フォーマットBcertを含んだ認証要求パケットを送信ノード9101に対して転送する（ステップS8502、S8702）。

【0235】これを受信した送信ノード9101は、送信ノードの認証フォーマットAcertを含んだ認証要求パケットを中継ノード9102に対して送信する（ステップS8503、S8602、S8603、S8703）。

【0236】次に、認証・鍵交換手続きを行って、送信ノード9101と中継ノード9102の両者で、認証鍵Kauth1を秘密裏に共有する（ステップS8504、S8505、S8604、S8704）。

【0237】IEEE1394著作権保護方式では、コンテンツ鍵Kは、交換鍵Kx、シードNc、暗号制御情報EMIの3つの変数の関数Jにて計算される。すなわち、 $K=J(Kx, Nc, EMI)$ である。ここでEMIは転送される暗号化データには必ず付与される値である。よって、送信ノード9101は、受信側（中継ノード、本実施形態の場合は無線ノードも）に対して、交換鍵KxとシードNcの値を通知する必要がある。

【0238】そこで、送信ノード9101は、中継ノード9102との間で共有した認証鍵Kauth1を使って、既知の関数fを使って、 $f(Kx, Kauth)$ の形で中継ノード9102に送信する（ステップS8506、S8605、S8708、S8709）。中継ノード9102は、この値から、Kxの値を算出することができる。同様に、シードNcの値も、送信ノード9101から中継ノード9102に転送される（ステップS8

507, S8606, S8710)。ここで、中継ノード9102は、暗号を復号するコンテンツ鍵Kを生成するのに必要なKx, Ncの値をこの時点で認識したことになる。

【0239】さて、同様の手続きが中継ノード9102と無線ノード9103の間でも行われる(ステップS8510~S8513, S8705~S8707, S8802~S8804)。この手続きは、送信ノード9101と中継ノード9102との間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ここで、無線網の無線同期チャネル#y上を転送される暗号化されたデータにも、送信元ノードである中継ノード9102を識別できるようなアドレス情報等が付与されていてもよい。

【0240】さて、中継ノード9102と無線ノード9101とで認証鍵Kauth2が共有できたものとする。本実施形態では、中継ノード9102は、暗号化されたMPEG映像を暗号の復号化をすることなく、そのまま無線網(の無線同期チャネル#y)にフォワード処理を行ってしまうため、中継ノード9102は無線ノード9103に対して、IEEE1394区間と同じ交換鍵KxとシードNcの値を通知する必要がある(逆に通知できれば、無線ノード9103は暗号の復号化が可能である。ただし、IEEE1394区間と無線網区間は、同じコンテンツ保護ポリシーで運営されているものとする)。そこで、中継ノード9102は、S8506, S8507で受信したデータより算出したKx, Ncのそれぞれの値を、同様に無線ノード9103に対して送信する(ステップS8514, S8515, S8709, S8711, S8805~S8807)。具体的には、Kxの値は認証鍵Kauth2の値を使って $f(Kx, Kauth2)$ を計算して、無線ノード9103に送出し、Ncの値はそのまま転送する。

【0241】無線ノード9103では、このようにして、中継ノードと同じ手順を使ってKx, Ncの値を認識できるため、同様の関数Jを使ってコンテンツ鍵Kの値を算出することができる(ステップS8516)。

【0242】よって、送信ノード9101から送られてくる、コンテンツ鍵Kで暗号化されたMPEG映像は、中継ノード9102で暗号の復号化がなされず、そのままフォワードして無線ノード9103まで転送されてきた場合(ステップS8508, S8517, S8607, S8712, S8809)でも、先にS8516で計算したコンテンツ鍵Kの値を使って、暗号の復号化ができる(ステップS8518, S8810)。その後、MPEG映像のデコード、ディスプレイ表示等が行われる。

【0243】なお、本実施形態では、無線網上では無線同期チャネルが定義されており、暗号化されたMPEG映像はこの無線同期チャネル上を転送されてくるとして

説明を行ってきたが、第2の実施形態のように、無線網上でのQOSデータ転送がイーサネットと同様の無線フレームを転送する場合にも、同様の方法(Kx, Ncの値を中継ノードから無線ノードにフォワードする)が適用可能である。

【0244】逆に言うと、本実施形態のような方法により、中継ノード9102では暗号の復号化および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【0245】なお、この場合、IEEE1394側に送信ノード9102とは別のノード(別ノード)が存在しており、この別ノードから中継ノード9102を経て、無線ノード9103に別のコンテンツ鍵で暗号化されたデータ(厳密には同じEMIを持ったデータ)を送信することはできない。コンテンツ鍵は、基本的にデータの送信ノード9101が決定する仕組みとなっていることから、別ノードが別のコンテンツ鍵を選択する可能性は十分にある。しかし、中継ノード9102と無線ノード9103との間で、既にコンテンツ鍵Kが一意に定義されている。すなわち、中継ノード9102と無線ノード9103との間では、同じEMI値については、1つのコンテンツ鍵しか共有できない。よって、両ノード間では、高々1つのコンテンツ鍵しか使うことができないため、別ノードからの(別のコンテンツ鍵で暗号化された)データを受信しても、これを中継ノード9102から無線ノード9103に転送する際に、別のコンテンツ鍵を生成できないため、これを復号化できないことになる。

【0246】よって、中継ノード9102は、既に暗号化データを送信しているノード(本実施形態の場合、無線ノード9103)に対して、別のコンテンツ鍵を使う必要のある暗号化データの送信要求があった場合(例えば、IEEE1394の別ノードの代理サービスに対するサービス要求があった場合等)は、これを拒否することにより、未然に上記矛盾を回避することが可能となる。また、中継ノード9102は、既に無線ノード9103に対して暗号化データの送信を行っている場合には、該無線ノード9103に対しては、他のサービス(サブユニット)は見せない(代理サービス提供自体を中断する、あるいは暗号化ストリーム転送を伴う代理サービスの提供を中断する、等)、というやり方でも、同様の効果が考えられる。

【0247】(第7の実施形態)第6の実施形態では、認証・鍵交換の単位を送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間でそれぞれ行ない、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いような方法であった。

【0248】これに対し、第7の実施形態では、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いのは同様であるが、無線網側での認証・鍵交換の単

位が、第2の実施形態と同じくサブユニット単位にでき、同じノード間でも複数のコンテンツ鍵を持つことができるような場合である。本実施形態によれば、IEEE 1394上の複数送信ノードからの暗号化データの同時受信が可能となる。

【0249】図87に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は、送信ノード(PとQ)が2つある点以外、基本的には第6の実施形態と同様である。

【0250】送信ノード9801、9811の内部構成は、第6の実施形態と同様である。

【0251】中継ノード9802の内部構成は、IEEE 1394側では認証・鍵交換の単位がノード間であり、無線側では認証・鍵交換の単位がサブユニット間である点を除いて、第6の実施形態と同様である。

【0252】無線ノード9803の内部構成は、認証・鍵交換の単位がサブユニット間である点を除いて、第6の実施形態と同様である。

【0253】なお、送信ノード9801、9811、無線ノード9802の動作手順は基本的には第6の実施形態と同様である。また、1つの送信ノードに対して中継を行う場合の中継ノード9803の動作手順も基本的には第6の実施形態と同様である。

【0254】これまでの実施形態と同様に、中継ノードでは、IEEE 1394側には無線網上のサービスの、無線側にはIEEE 1394上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【0255】次に、複数の送信ノードに対して中継を行う場合の中継ノード9802の動作手順例を図88に、本実施形態の全体のシーケンス例を図89/図90に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス(映像送信サブユニット)を代理で無線側に広告しており、無線ノード(の映像デコードサブユニット)が、中継ノードの代理機能に対してサービス(MPEG映像転送要求)を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でIEEE 1394上は同期チャンネル#x上を、無線上は無線同期チャンネル#y上を転送されるものとする。詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【0256】本実施形態でも、IEEE 1394上の著作権保護方式である「5C Digital Transmission Content Protection Specification」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。

【0257】さて、送信ノードP(9801)は、IEEE 1394の同期チャンネル#x上に、コンテンツ鍵K

1で暗号化されたMPEG映像を転送する(ステップS9201、S9301)。第6の実施形態と同様に、コンテンツ鍵K1は、 $K1 = J(Kxp, Ncp, EM1)$ にて計算されるものとする。これを受信した中継ノード9802は、このまま(受信したMPEG映像を、コンテンツ鍵K1で暗号化されたまま)無線側の無線同期チャンネル#yに対して転送する(ステップS9209、S9301)。

【0258】中継ノード9802が送信ノードPに対して認証要求をし、鍵交換などを行って、交換鍵KxpとシードNcpを獲得する手順(ステップS9202~S9207、S9302)は、第6の実施形態と同様であるので、ここでの詳細な説明は省略する。この時点で、中継ノード9802は暗号を復号するために必要なKxp、Ncpの値を認識したことになる。

【0259】さて、同様の認証・鍵交換手続きが中継ノード9802と無線ノード9803の間でも行われる(ステップS9210~S9217、S9303)。この手続きは第2の実施形態の送信ノードと中継ノード間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ただし、認証先問い合わせや認証先応答、あるいは認証要求にサブユニットのIDの他、チャンネル番号、あるいは暗号化データの送受信を行うことになるプラグの識別子を搭載して、これを行ってもよい。中継ノード9802、あるいは無線ノード9803が、「どの暗号化データについての認証・鍵交換手続きか」ということが識別できるようになり、後述するように、異なる鍵の暗号化データについては、同一のノード間の認証・鍵交換であったとしても、異なる鍵を通知することが可能になる。

【0260】なお、この際、認証要求にチャンネル番号を含める場合は、ステップS9210の認証先問い合わせとステップS9211の認証先応答は不要となる。

【0261】さて、中継ノード9802と無線ノード9803で認証鍵Kauth1が共有できたものとする。本実施形態でも、中継ノード9802は、暗号化されたMPEG映像を暗号の復号化をすることなく、そのまま無線網(の無線同期チャンネル#y)にフォワード処理を行ってしまうため、中継ノード9802は無線ノード9803に対して、交換鍵KxpとシードNcpの値を通知する必要がある(逆に通知できれば、無線ノード9803は暗号の復号化が可能である)。そこで、中継ノード9802は、S9206、S9207で受信したデータより算出したKxp、Ncpのそれぞれの値を、同様に無線ノード9803に対して送信する(ステップS9216、S9217)。Kxpの値は認証鍵Kauth1の値を使って $f(Kxp, Kauth1)$ を計算して、無線ノード9803に送出する(ステップS9216)。

【0262】無線ノード9803では、このようにし

て、中継ノード9802と同じ手順を使って $K_{xp}$ 、 $N_{cp}$ の値を認識できるため、同様の関数 $J$ を使ってコンテンツ鍵 $K_1$ の値を算出することができる(ステップS9218)。

【0263】よって、送信ノードPから送られてくる、コンテンツ鍵 $K_1$ で暗号化されたMPEG映像は、中継ノード9802で暗号の復号化をせずに、そのままフォワードして無線ノード9803まで転送されてきた場合(ステップS9208、S9219)でも、先にステップS9218で計算したコンテンツ鍵 $K_1$ の値を使って、暗号の復号化ができる(ステップS9220)。その後、MPEG映像のデコード、ディスプレイ表示等が行われる。

【0264】本実施形態のような方法でも、中継ノード9802では暗号の復号化、および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【0265】さて、次に、別の送信ノードQ(9811)が、同時に中継ノード9802を介して無線ノード9803に対して別のコンテンツ鍵 $K_2$ で暗号化されたデータを送信する場合(ステップS9221、S9229、S9304)を考える。

【0266】本実施形態の前半と同様に、送信ノードQと中継ノード9802との間で認証・鍵交換が行われ(ステップS9222～S9227)、中継ノード9802は交換鍵 $K_{xq}$ とシード $N_{cq}$ の値をそれぞれ得ることができる。

【0267】本実施形態においては、中継ノード9802と無線ノード9803との間の認証は、サブユニット間単位であるので、暗号化データの送受が異なるサブユニット間で行われているものとすれば、中継ノード9802と無線ノード9803との間で複数の認証・鍵交換が可能となる。

【0268】すなわち、本実施形態の前半と同様に、中継ノード9802と無線ノード9803との間で、本実施形態の前半とは異なるサブユニット間で認証・鍵交換を行っていく(ステップS9230～S9235、S9305)。その上で、中継ノード9802は、送信ノードQと自ノード(中継ノード)9802との間の交換鍵 $K_{xq}$ とシード $N_{cq}$ を、無線ノード9803にフォワードする(ステップS9236、S9237、S9305、S9306)。

【0269】無線ノード9803では、このようにして、 $K_{xq}$ 、 $N_{cq}$ の値を認識できるため、同様の関数 $J$ を使ってコンテンツ鍵 $K_2$ の値を算出することができる(ステップS9238)。

【0270】よって、送信ノードQから送られてくる、コンテンツ鍵 $K_2$ で暗号化されたMPEG映像は、中継ノード9802で暗号の復号化をせずに、そのままフォワードして無線ノード9803まで転送されてきた場合

(ステップS9228、S9229)でも、先にステップS9238で計算したコンテンツ鍵 $K_2$ の値を使って、暗号の復号化ができる(ステップS9240)。つまり、2つの異なるコンテンツ鍵(本実施形態では $K_1$ と $K_2$ )で暗号化されたMPEG映像の同時受信が可能となる。

【0271】なお、第6の実施形態と第7の実施形態では、IEEE1394と無線網との相互接続を行う場合を例に説明してきたが、インターネット等のその他の網についても適用可能である。

【0272】なお、第1～第7の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合(例えば、無線ノードからIEEE1394上のノードへデータ転送する場合)にも、本発明は適用可能である。

【0273】また、第1～第7の実施形態において、無線ノードやIEEE1394上のノードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードやIEEE1394上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

【0274】また、認証手続きや、鍵交換手続き(コンテンツ鍵共有手続き)は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【0275】また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【0276】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0277】また、本実施形態は、コンピュータに所定の手段を実行させるための(あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための)プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0278】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0279】

【発明の効果】本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るネットワークの全体構成の一例を示す図

【図2】送信ノードの内部構造の一例を示す図

【図3】中継ノードの内部構造の一例を示す図

【図4】無線ノードの内部構造の一例を示す図



【図5】全体のシーケンスの一例を示す図  
【図6】全体のシーケンスの一例を示す図  
【図7】送信ノードの動作手順の一例を示すフローチャート  
【図8】送信ノードの動作手順の一例を示すフローチャート  
【図9】中継ノードの動作手順の一例を示すフローチャート  
【図10】中継ノードの動作手順の一例を示すフローチャート  
【図11】中継ノードの動作手順の一例を示すフローチャート  
【図12】無線ノードの動作手順の一例を示すフローチャート  
【図13】無線ノードの動作手順の一例を示すフローチャート  
【図14】無線ノード構成情報パケットの一例を示す図  
【図15】代理テーブルの一例を示す図  
【図16】代理テーブルの一例を示す図  
【図17】送信ノードから見た中継ノードの内部構造を説明するための図  
【図18】無線ノードから見た中継ノードの内部構造を説明するための図  
【図19】無線ノード制御パケットの一例を示す図  
【図20】本発明の第2の実施形態に係るネットワークの全体構成の一例を示す図  
【図21】送信ノードの内部構造の一例を示す図  
【図22】中継ノードの内部構造の一例を示す図  
【図23】無線ノードの内部構造の一例を示す図  
【図24】全体のシーケンスの一例を示す図  
【図25】全体のシーケンスの一例を示す図  
【図26】送信ノードの動作手順の一例を示すフローチャート  
【図27】送信ノードの動作手順の一例を示すフローチャート  
【図28】中継ノードの動作手順の一例を示すフローチャート  
【図29】中継ノードの動作手順の一例を示すフローチャート  
【図30】中継ノードの動作手順の一例を示すフローチャート  
【図31】中継ノードの動作手順の一例を示すフローチャート  
【図32】無線ノードの動作手順の一例を示すフローチャート  
【図33】無線ノードの動作手順の一例を示すフローチャート  
【図34】代理テーブルの一例を示す図  
【図35】代理テーブルの一例を示す図  
【図36】送信ノードから見た中継ノードの内部構造を

説明するための図

【図37】無線ノードから見た中継ノードの内部構造を説明するための図

【図38】無線フレームのフォーマットの一例を示す図

【図39】無線制御パケットのフォーマットの一例を示す図

【図40】本発明の第3の実施形態に係るネットワークの全体構成の一例を示す図

【図41】送信ノードの内部構造の一例を示す図

【図42】中継ノードの内部構造の一例を示す図

【図43】無線ノードの内部構造の一例を示す図

【図44】全体のシーケンスの一例を示す図

【図45】全体のシーケンスの一例を示す図

【図46】送信ノードの動作手順の一例を示すフローチャート

【図47】送信ノードの動作手順の一例を示すフローチャート

【図48】中継ノードの動作手順の一例を示すフローチャート

【図49】中継ノードの動作手順の一例を示すフローチャート

【図50】中継ノードの動作手順の一例を示すフローチャート

【図51】無線ノードの動作手順の一例を示すフローチャート

【図52】無線ノードの動作手順の一例を示すフローチャート

【図53】代理テーブルの一例を示す図

【図54】代理テーブルの一例を示す図

【図55】送信ノードから見た中継ノードの内部構造を説明するための図

【図56】無線ノードから見た中継ノードの内部構造を説明するための図

【図57】無線ノードに送られてきた制御画面の一例を示す図

【図58】本発明の第4の実施形態に係るネットワークの全体構成の一例を示す図

【図59】送信ノードの内部構造の一例を示す図

【図60】ホームゲートウェイの内部構造の一例を示す図

【図61】受信ノードの内部構造の一例を示す図

【図62】全体のシーケンスの一例を示す図

【図63】全体のシーケンスの一例を示す図

【図64】送信ノードの動作手順の一例を示すフローチャート

【図65】送信ノードの動作手順の一例を示すフローチャート

【図66】ホームゲートウェイの動作手順の一例を示すフローチャート

【図67】ホームゲートウェイの動作手順の一例を示す

フローチャート

【図68】ホームゲートウェイの動作手順の一例を示すフローチャート

【図69】ホームゲートウェイの動作手順の一例を示すフローチャート

【図70】受信ノードの動作手順の一例を示すフローチャート

【図71】受信ノードの動作手順の一例を示すフローチャート

【図72】送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図

【図73】本発明の第5の実施形態に係るネットワークの全体構成の一例を示す図

【図74】ホームゲートウェイの内部構造の一例を示す図

【図75】全体のシーケンスの一例を示す図

【図76】制御画面の一例を示す図

【図77】本発明の第6の実施形態に係るネットワークの全体構成の一例を示す図

【図78】送信ノードの内部構造の一例を示す図

【図79】中継ノードの内部構造の一例を示す図

【図80】無線ノードの内部構造の一例を示す図

【図81】全体のシーケンスの一例を示す図

【図82】送信ノードの動作手順の一例を示すフローチャート

【図83】中継ノードの動作手順の一例を示すフローチャート

【図84】中継ノードの動作手順の一例を示すフローチャート

【図85】無線ノードの動作手順の一例を示すフローチャート

【図86】無線ノードの動作手順の一例を示すフローチャート

【図87】本発明の第7の実施形態に係るネットワークの全体構成の一例を示す図

【図88】中継ノードの動作手順の一例を示すフローチャート

【図89】全体のシーケンスの一例を示す図

【図90】全体のシーケンスの一例を示す図

【符号の説明】

101, 2101, 4101, 6101, 8101, 9101, 9801, 9811…送信ノード

102, 2102, 4102, 9102, 9802…中継ノード

103, 2103, 4103, 6104, 9103, 9803…無線ノード

6102, 8102, 8103…ホームゲートウェイ

6103, 8104…受信ノード

104, 2104, 4104, 8105, 8107, 9104, 9804…IEEE1394バス

6105, 8106…公衆網

201, 2201, 4201, 6201, 8201, 9101…IEEE1394インタフェース

202, 2202, 4202, 9202…無線インタフェース

203, 2207, 4203, 6207, 8203, 9207…AV/Cプロトコル処理部

204, 2203, 4204, 6203, 8204, 9203…ISO信号送受信部

205, 2206, 4205, 9206…無線ISO信号送受信部

206, 2209, 4206, 6209, 9209…1394バス構成認識部

207, 2210, 4207, 8207, 9210…代理サブユニット構成部

208, 2214, 4208, 6215, 9214…代理テーブル

209, 2211, 4209, 9211…無線区間構成認識部

210, 4210, 8209…コピープロテクション制御/フォワード部

2208, 6208…IEEE1394コピープロテクション処理部

2212, 9212…無線区間コピープロテクション部

8211…変換テーブル

211, 2213, 4211, 9213…無線ノード制御パケット送受信部

2204, 6204…暗号復号化部

2205, 6205…暗号化部

4212…HAVi処理部

4213…IEEE1212レジスタ

6206, 8205…AV信号送受信部

6202, 8202…インターネットインタフェース

6210, 8208…代理ホームページ作成部

6211, 8210…ホームページ作成・蓄積部

6212…インターネット側プロテクション処理部

6213…制御パケット送受信部

6214…MPEG2/MPEG4変換部

6206…制御パケット処理信部

301, 2301, 4301, 9301…無線インタフェース

302, 2302, 4302, 9302…無線ノード制御パケット送受信部

303, 2303, 4303, 6303, 9303…コピープロテクション処理部

304, 2304, 4304, 9304…無線ISO信号送受信部

305, 2305, 4305, 6305, 9305…暗号復号化部

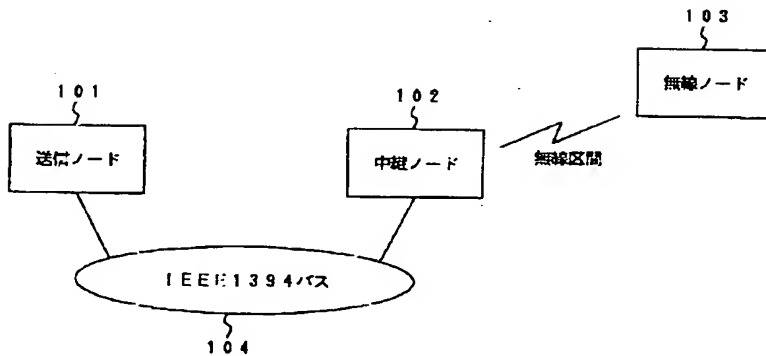
306, 2306, 4306, 6306, 9306…M



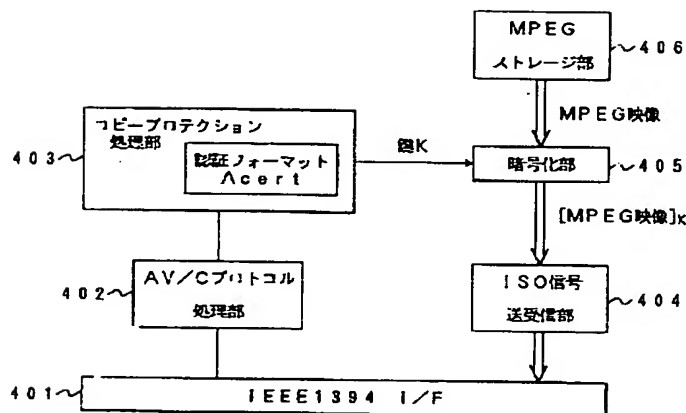
PEGデコード部  
 307, 2307, 4307, 6307, 9307…ディスプレイ部  
 6301…インターネットインタフェース  
 6302…制御パケット送受信部  
 6304…AV信号送受信部  
 401, 2401, 4401, 6401, 9401…IEEE1394インタフェース  
 402, 2402, 4402, 6402, 9402…AV/Cプロトコル処理部

403, 2403, 4403, 6403, 9403…コピープロテクション処理部  
 404, 2404, 4404, 6404, 9404…ISO信号送受信部  
 405, 2405, 4405, 6405, 9405…暗号化部  
 406, 2406, 4406, 6406, 9406…MPEGストレージ部  
 4407…IEEE1212レジスタ

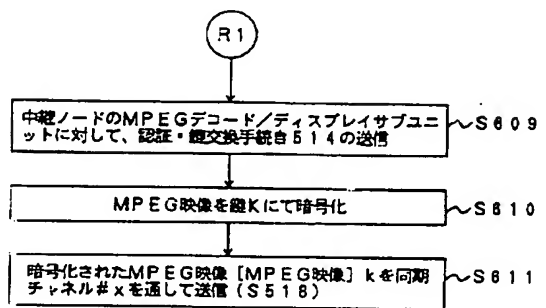
【図1】



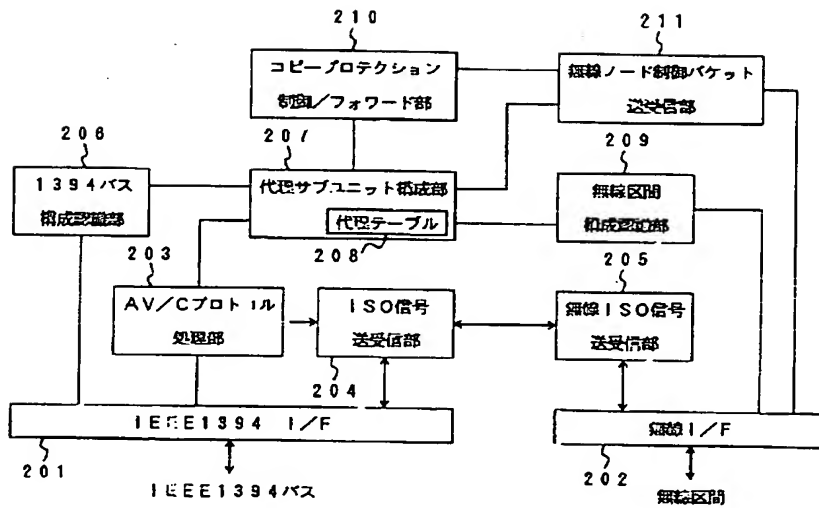
【図2】



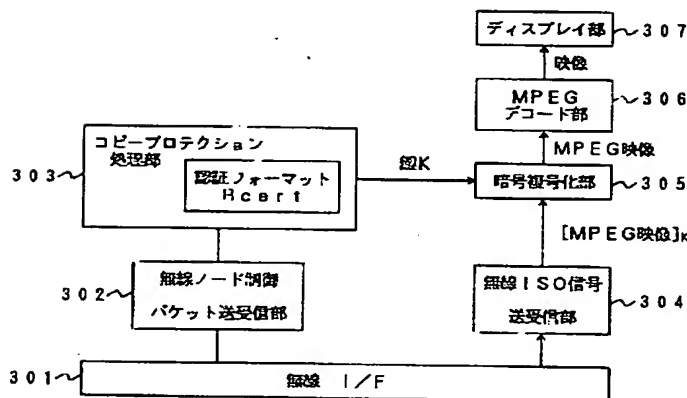
【図8】



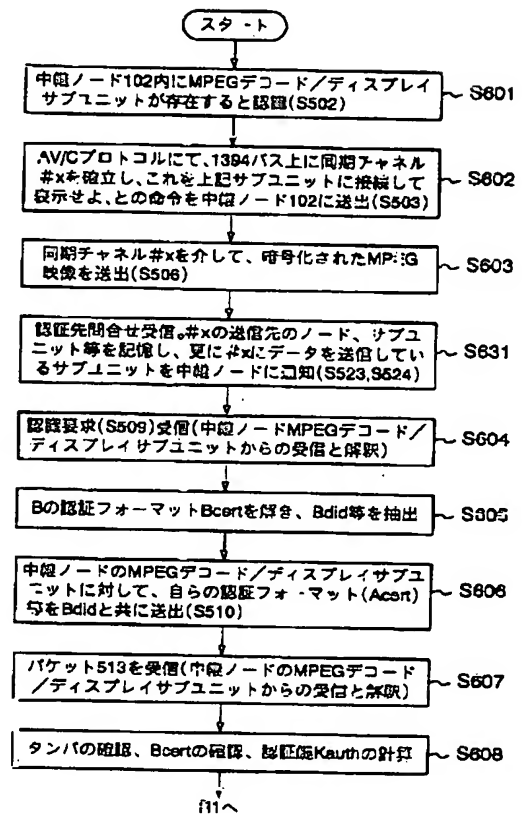
【図3】



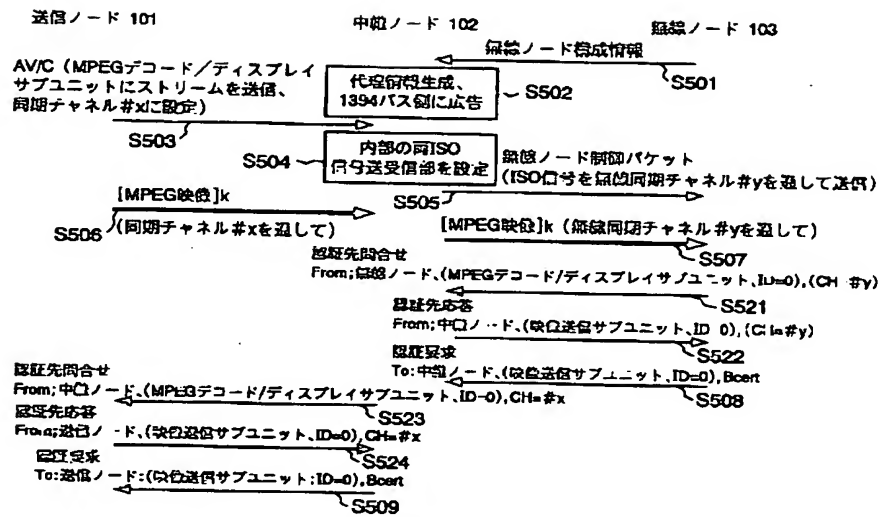
【図4】



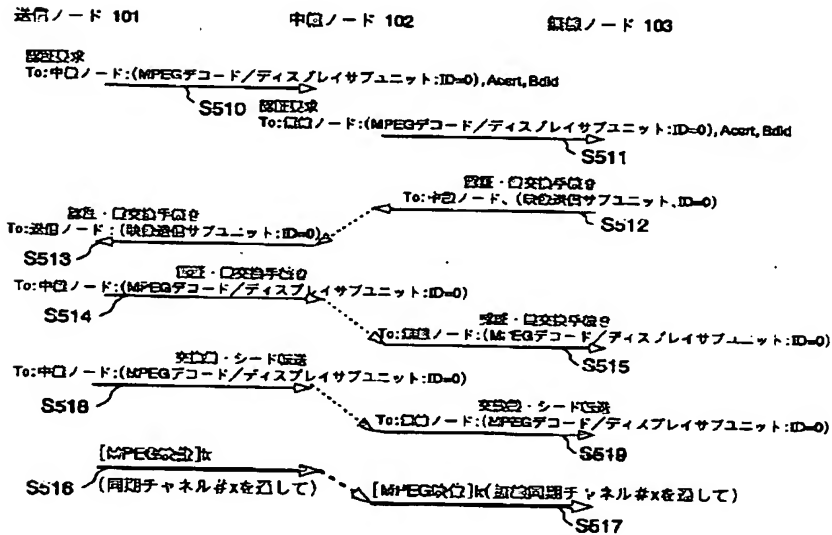
【図7】



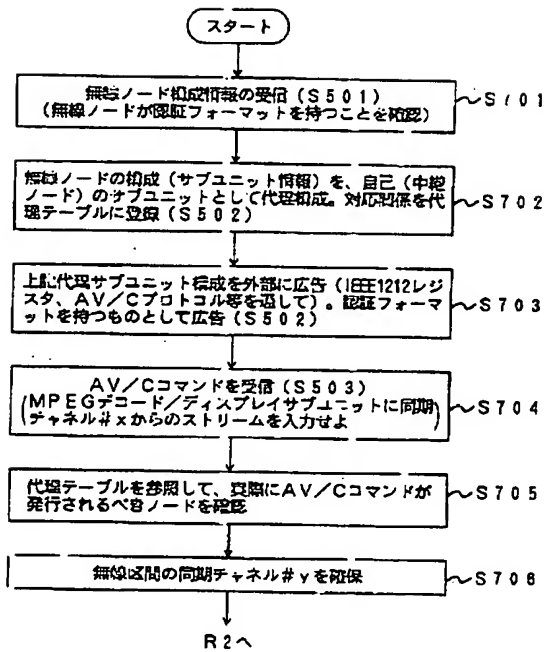
【図5】



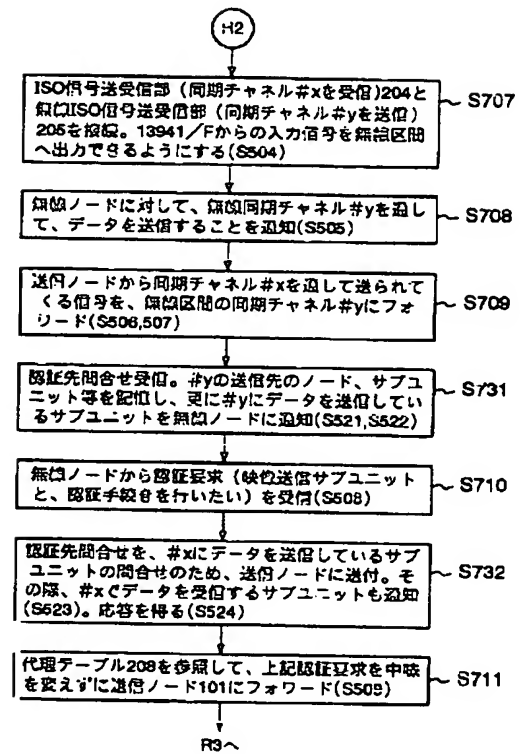
【図6】



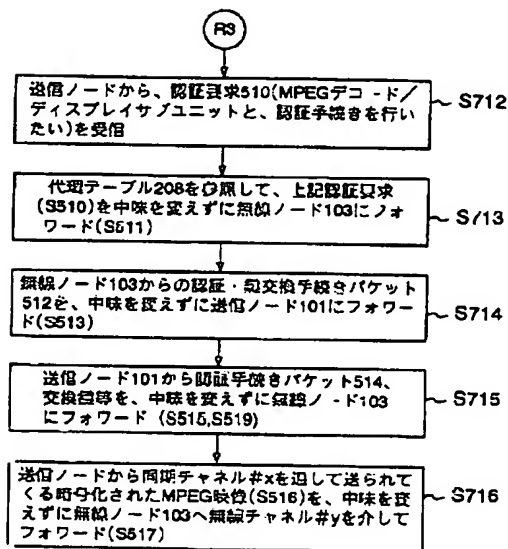
【図9】



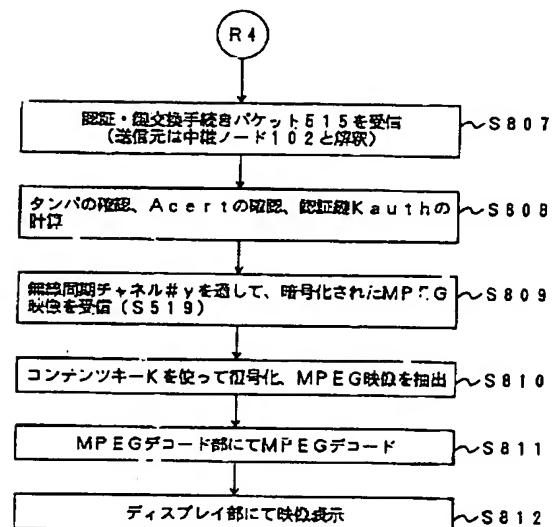
【図10】



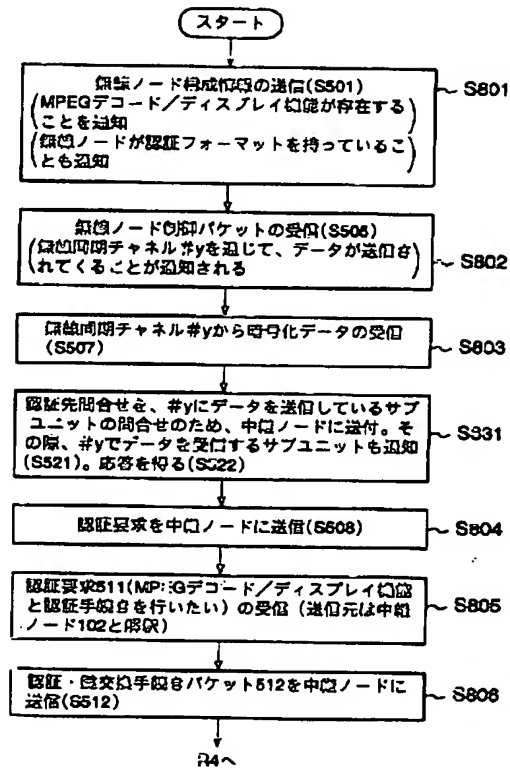
【図11】



【図13】



【図12】



【図14】

宛先ノード=中継ノード
送信元ノード=無線ノード
形成1=MPEGデコード/ディスプレイ機能
形成2=...
...
形成1の属性1=認証フォーマット (認証機能=...)
形成1の属性2=MPEGの上限ビットレート6Mbps
...

【図15】

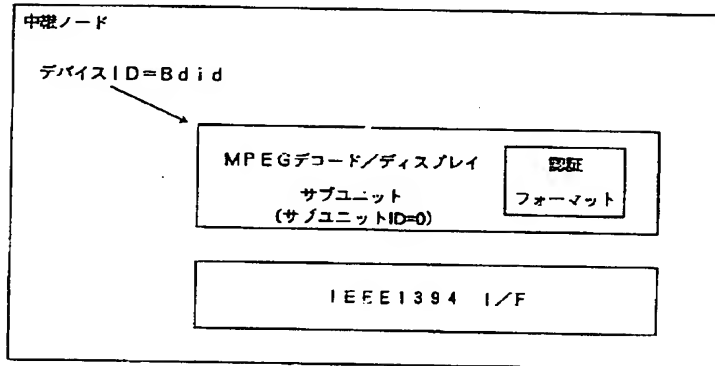
無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード103の MPEGデコード/ディスプレイ機能 (サブユニットID=0) (認証フォーマット有)	MPEGデコード/ディスプレイサブユニット (サブユニットID=0) (認証フォーマット有)
...	...

【図16】

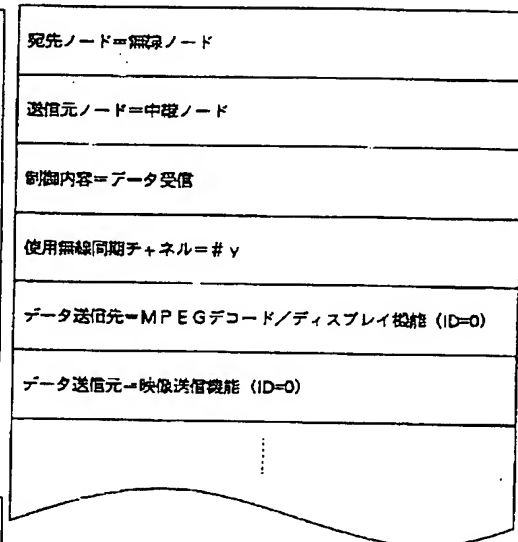
1394バス側の実体	中継ノードが無線区間側に代理サービスする形態	送信元アドレス
送信ノード101の映像送信機能 (映像送信サブユニット) (サブユニットID=0) (認証フォーマット有)	映像送信サブユニット (サブユニットID=0) (認証フォーマット有)	宛先アドレス
...	...	データ

【図38】

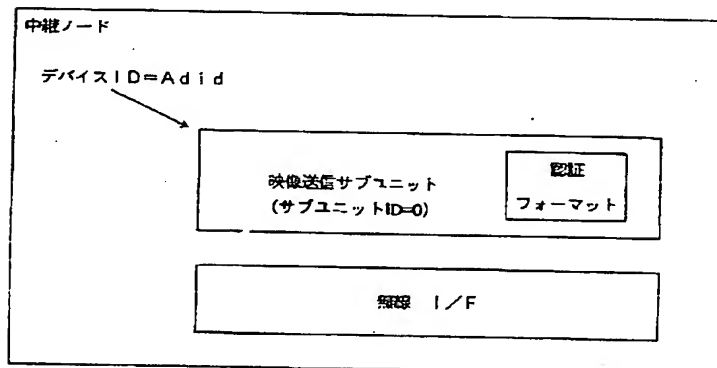
【図17】



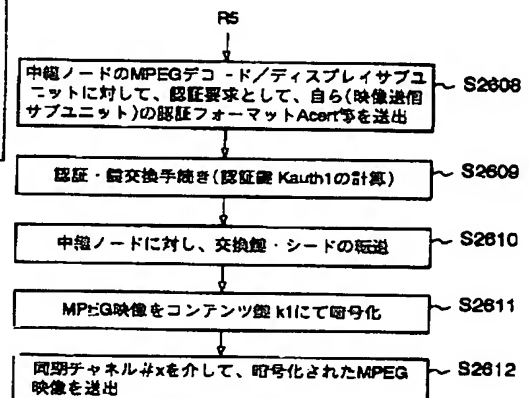
【図19】



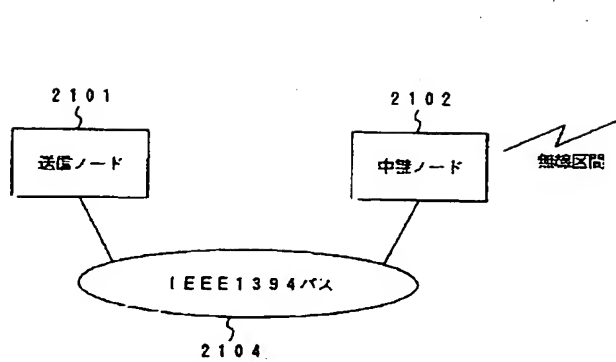
【図18】



【図27】



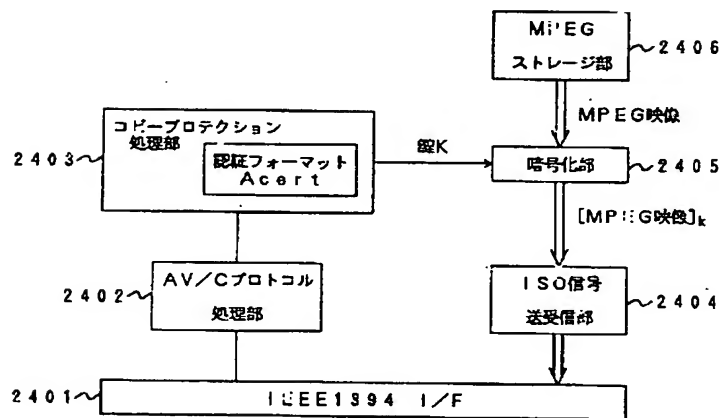
【図20】



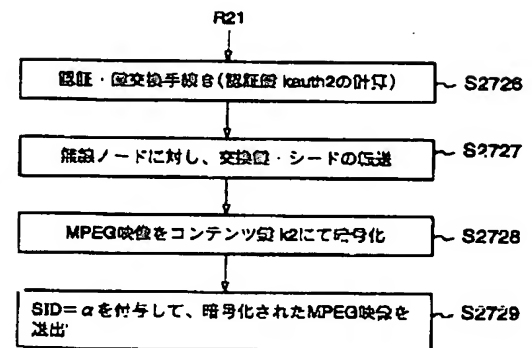
【図39】

宛先ノード=無線ノード
送信元ノード=中間ノード
制御内容=データ受信
使用SID= $\alpha$
データ送信元= MPEGデコード/ディスプレイ サブユニット(サブユニットID=0)
データ送信元= 映像送信サブユニット (サブユニットID=0)

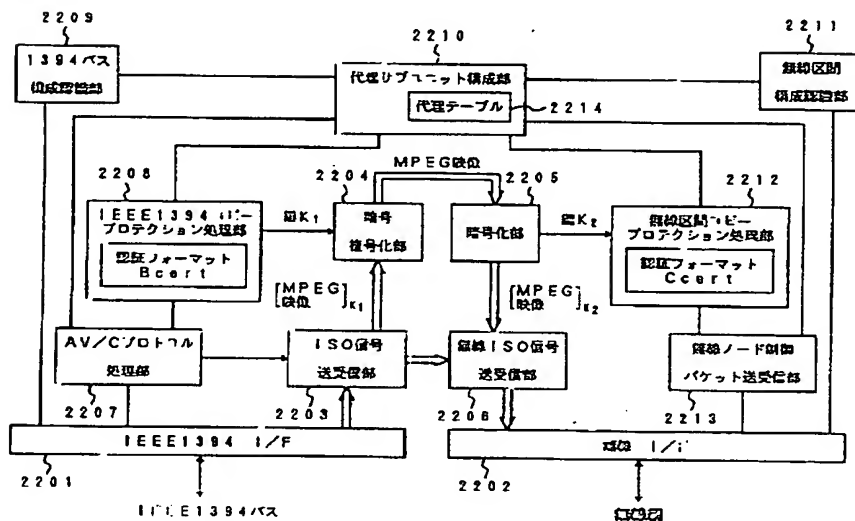
【図21】



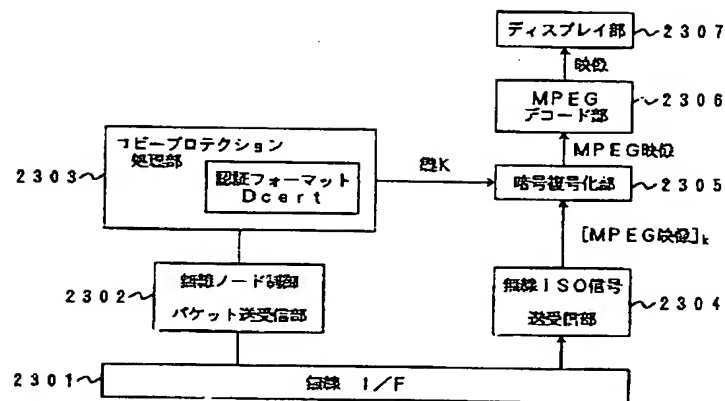
【図31】



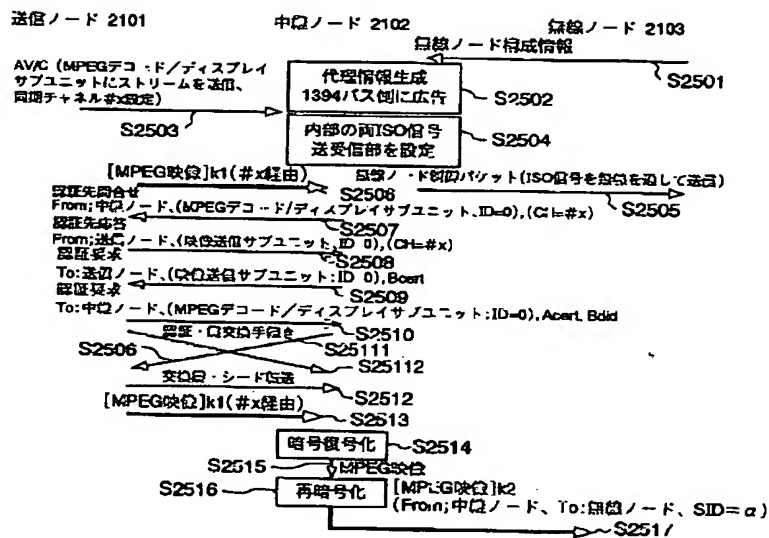
【図22】



【図23】

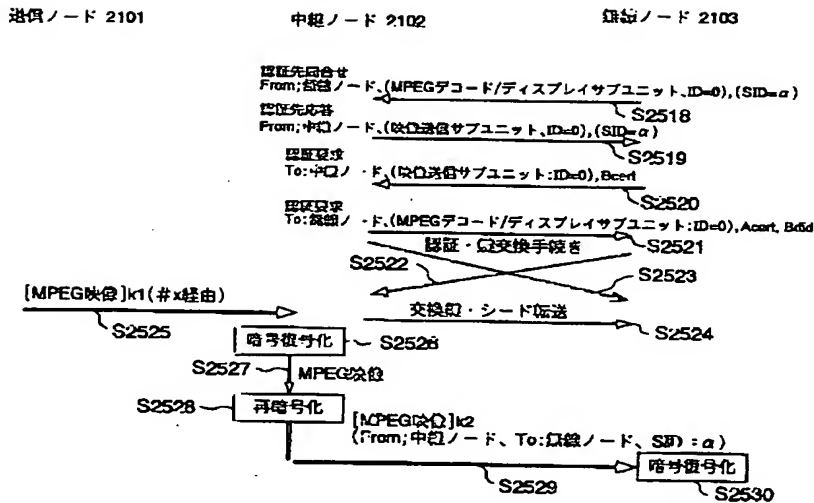


【図24】

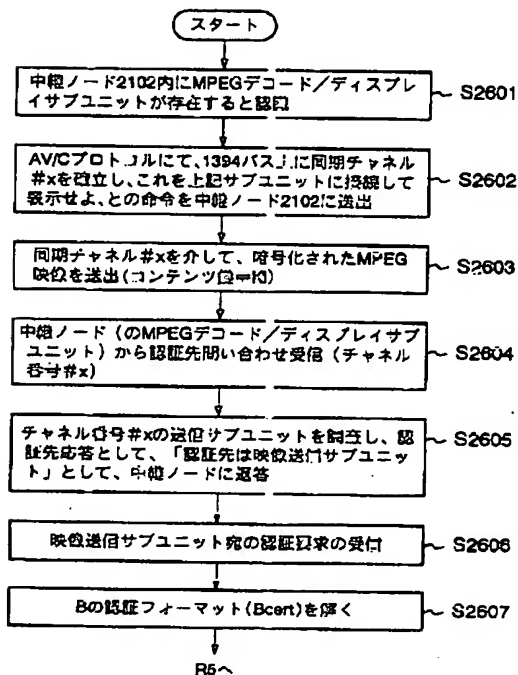




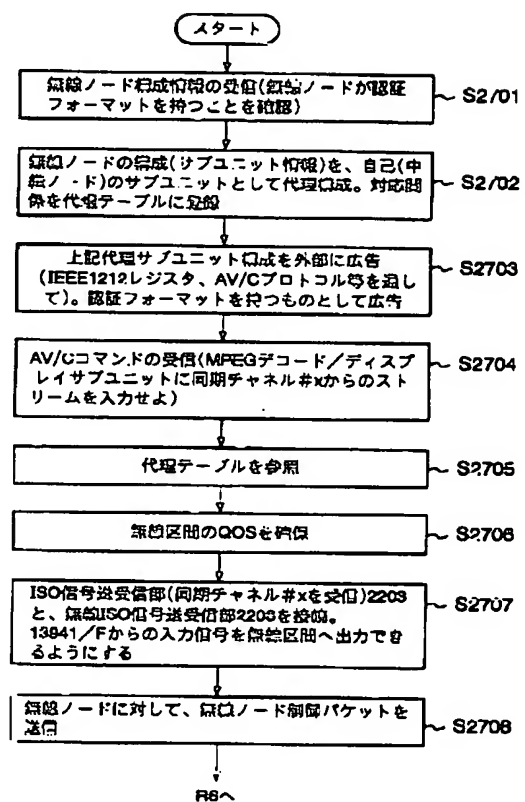
【図25】



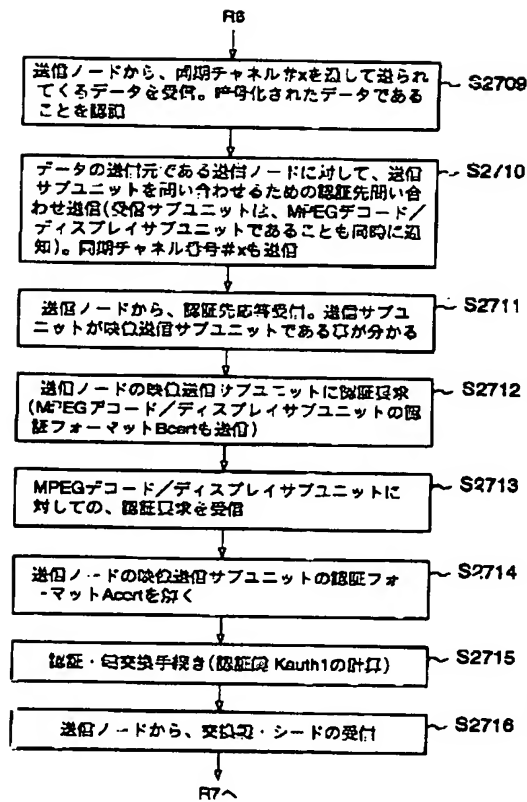
【図26】



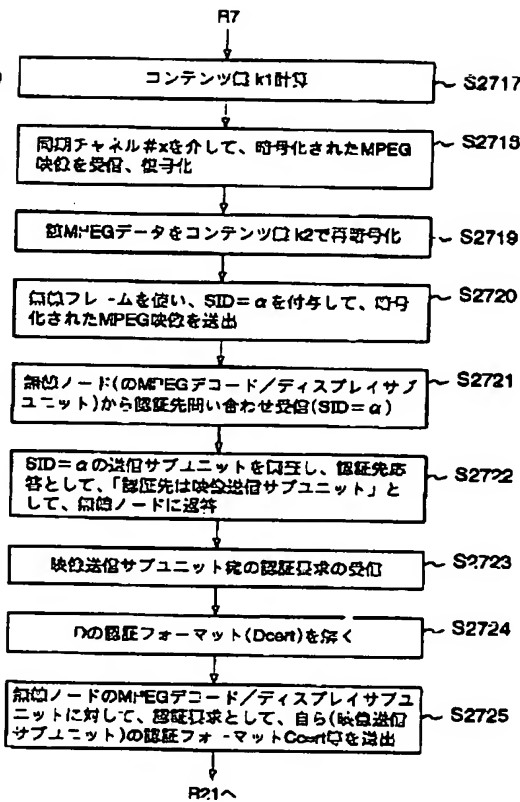
【図28】



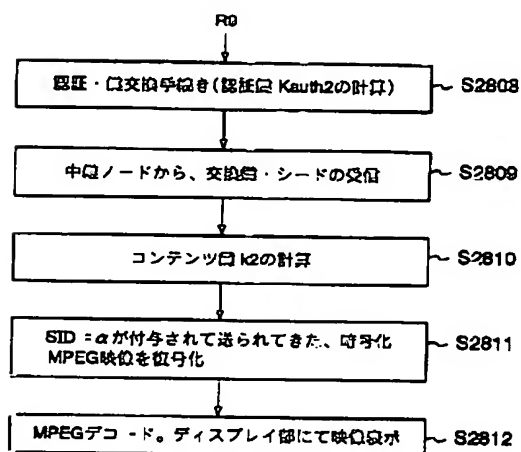
【図29】



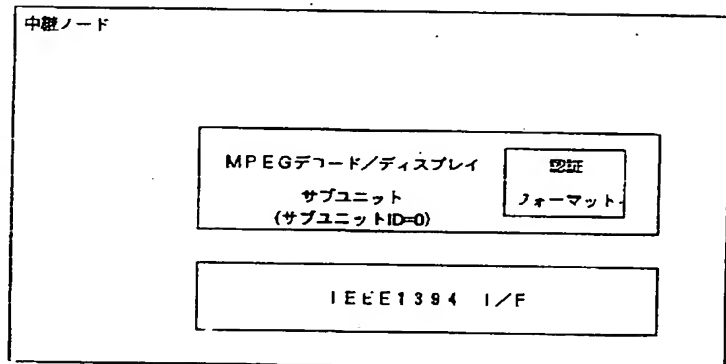
【図30】



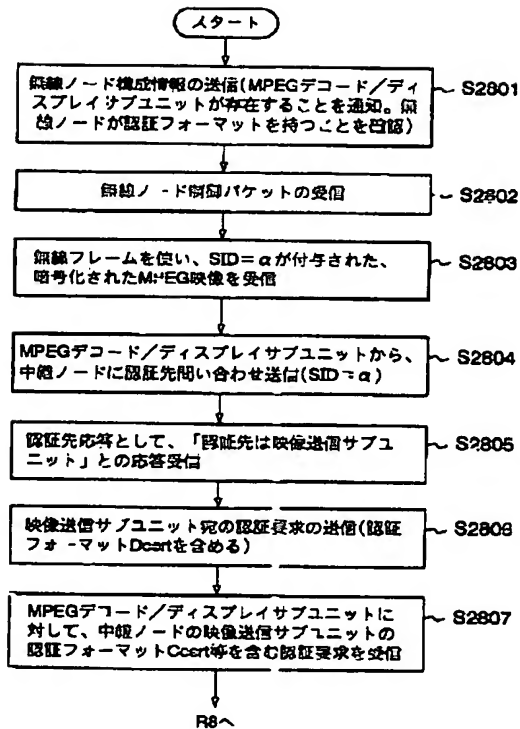
【図33】



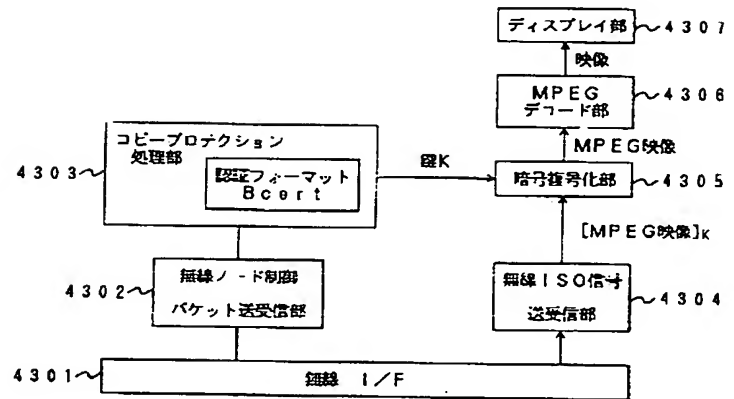
【図36】



【図32】



【図43】



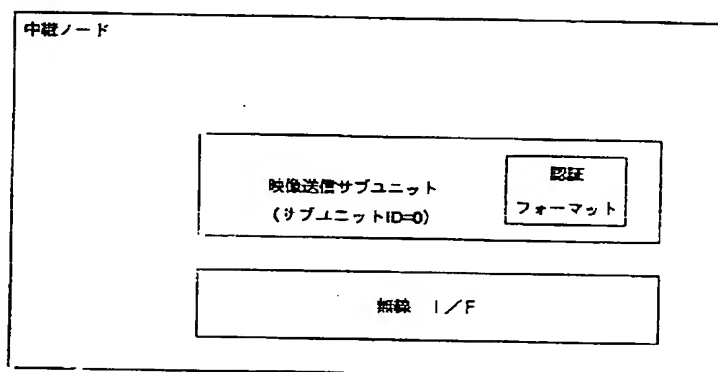
【図34】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード103の MPEGデコード/ディスプレイ機能 (サブユニットID=0)	MPEGデコード/ディスプレイサブユニット (サブユニットID=0)
⋮	⋮

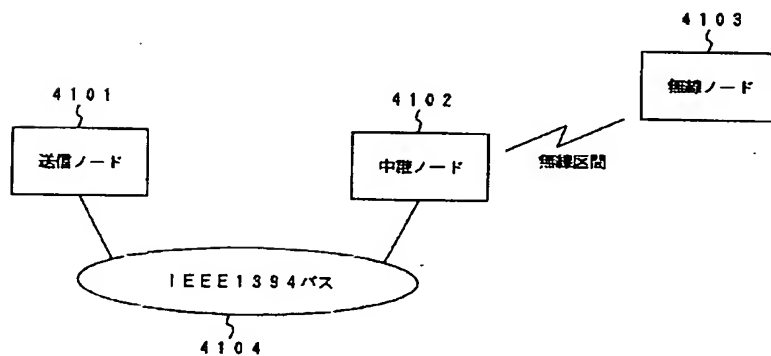
【図35】

1394バス側の変体	中継ノードが無線区間側に代理サービスする形態
送信ノード101の映像送信機能 (映像送信サブユニット) (サブユニットID=0)	映像送信サブユニット (サブユニットID=0)
...	...

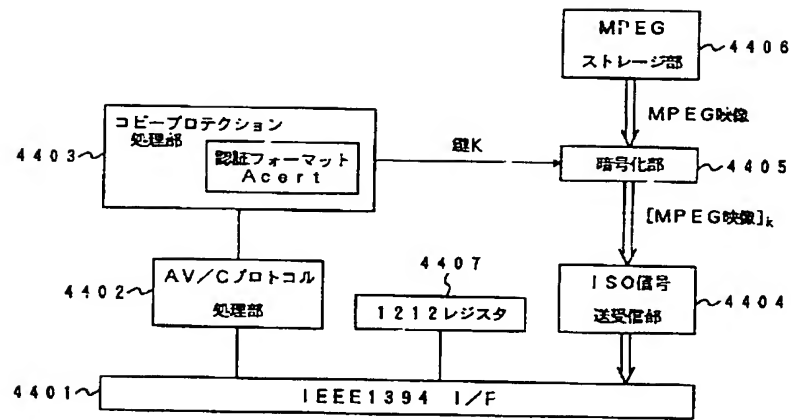
【図37】



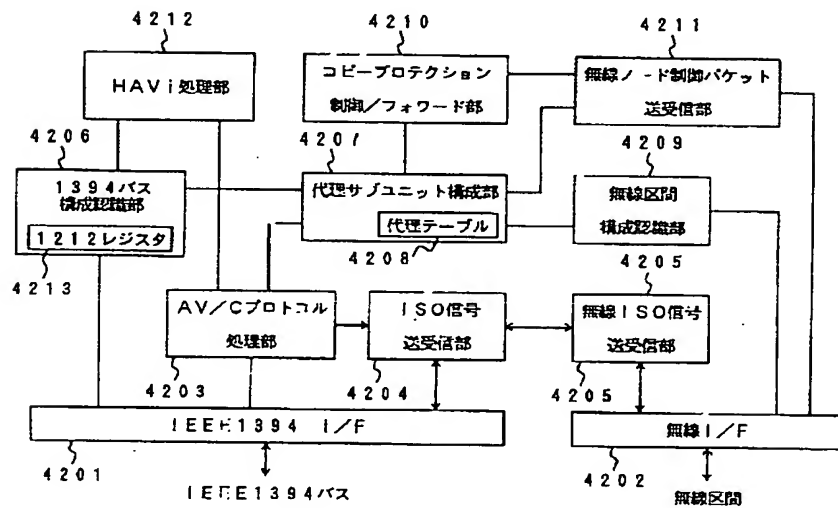
【図40】



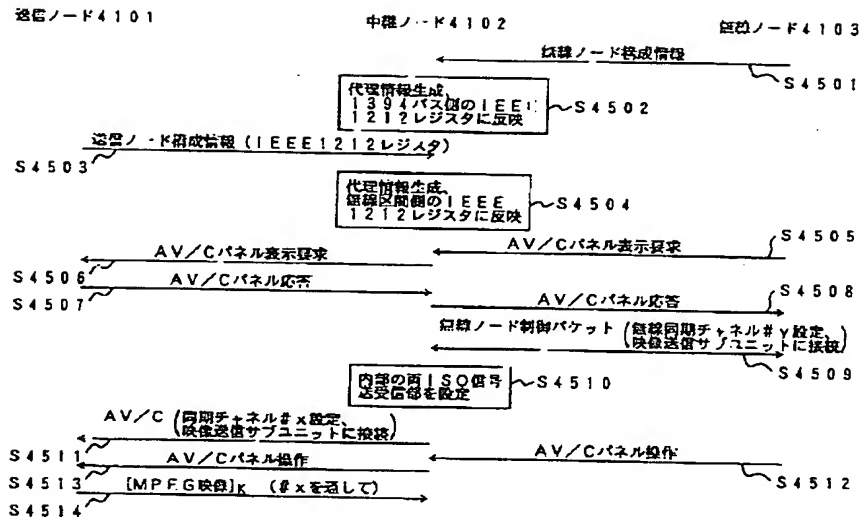
【図41】



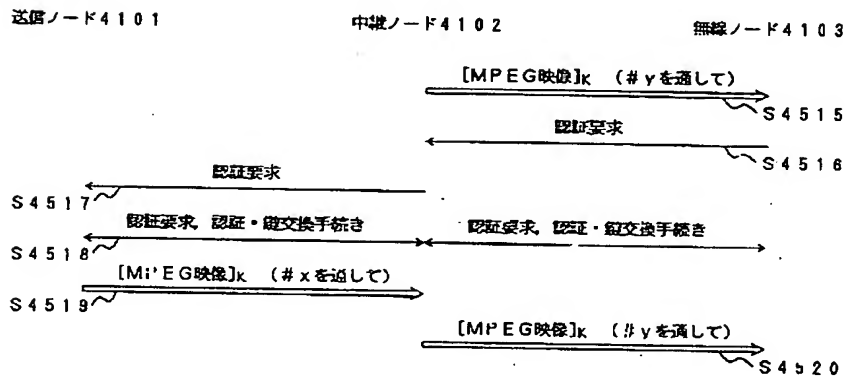
【図42】



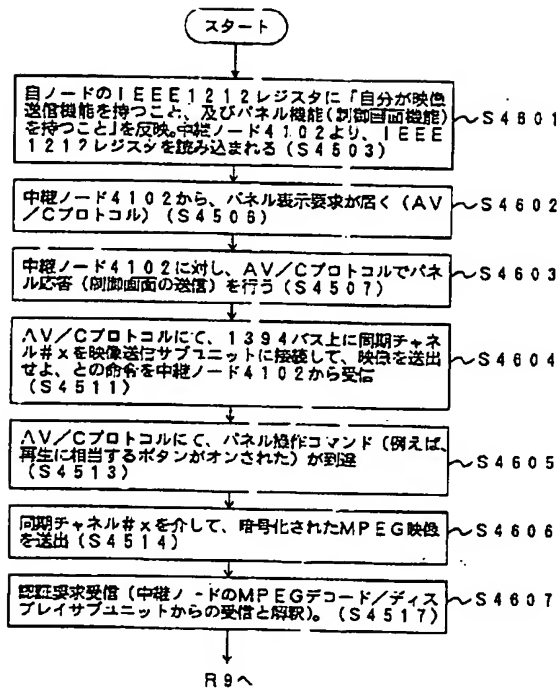
【図44】



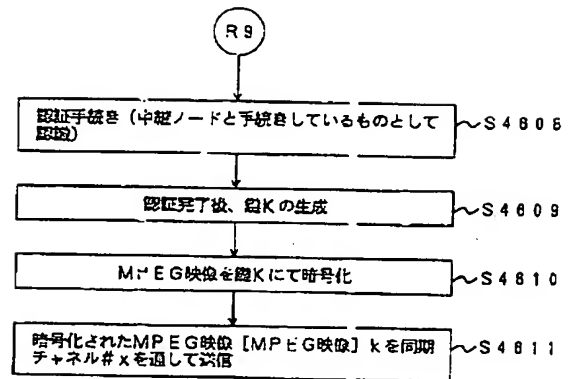
【図45】



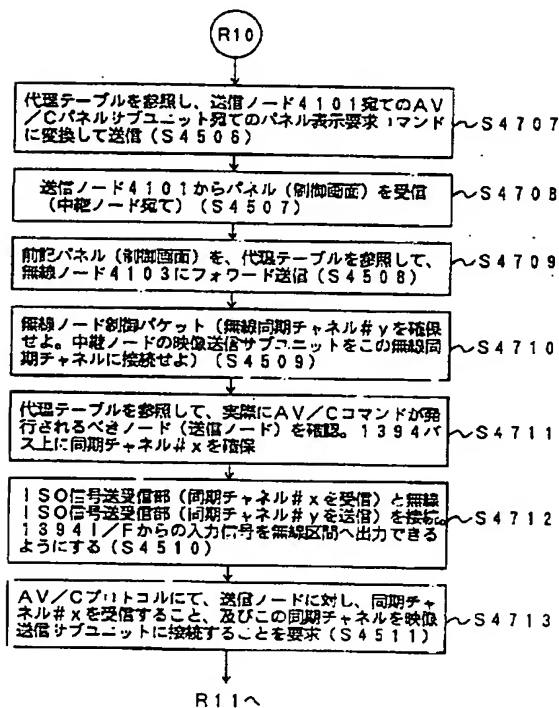
【図46】



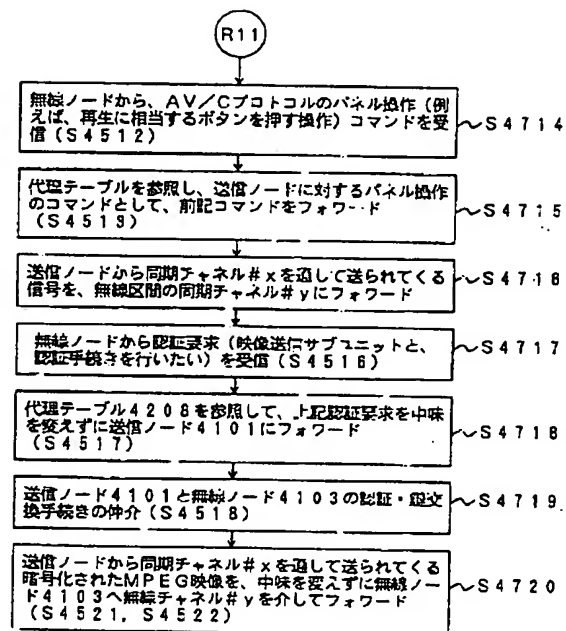
【図47】



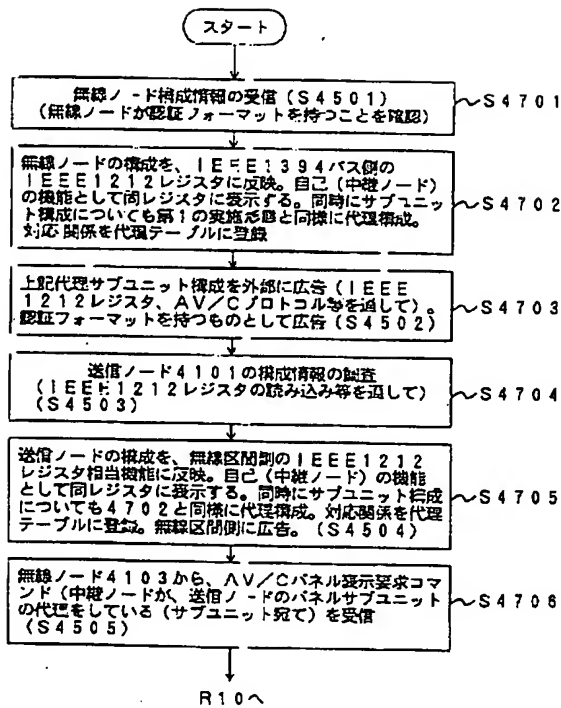
【図49】



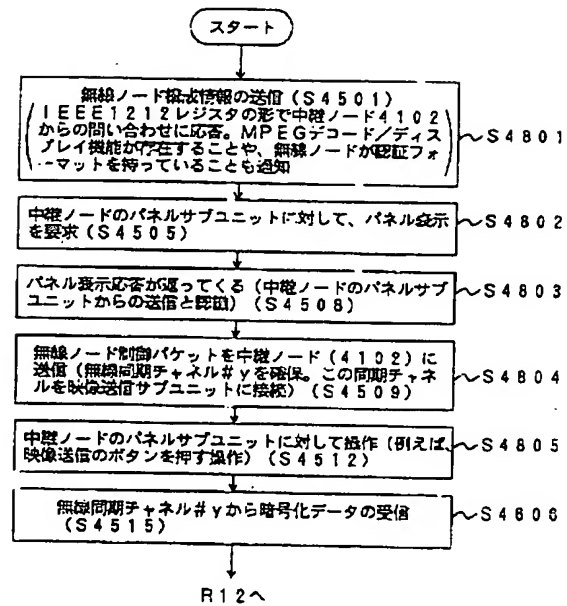
【図50】



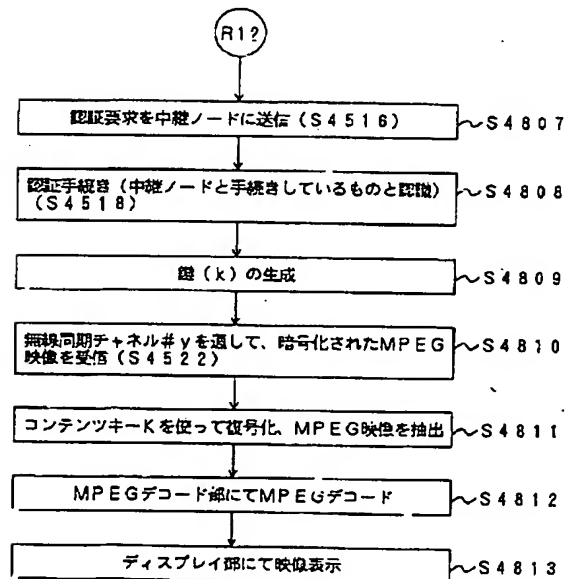
【図48】



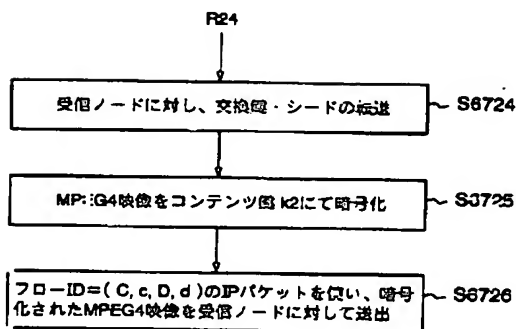
【図51】



【図52】



【図69】





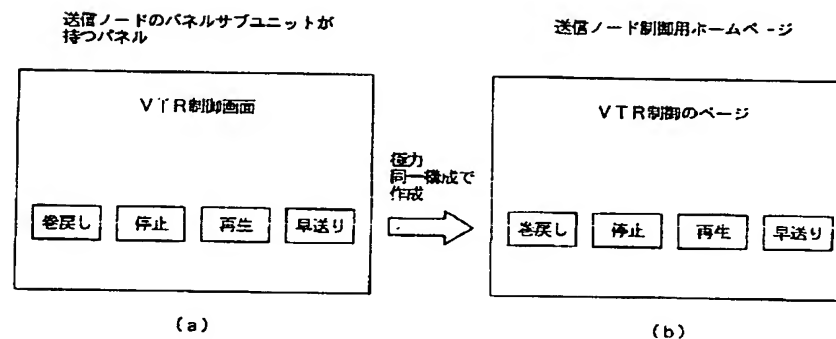
【図53】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード4103の MPEGデコード/ディスプレイ機能 (認証フォーマット有)	MPEGデコード/ディスプレイサブユニット (認証フォーマット有)
無線ノード4103のパネル機能	パネルサブユニット
⋮	⋮

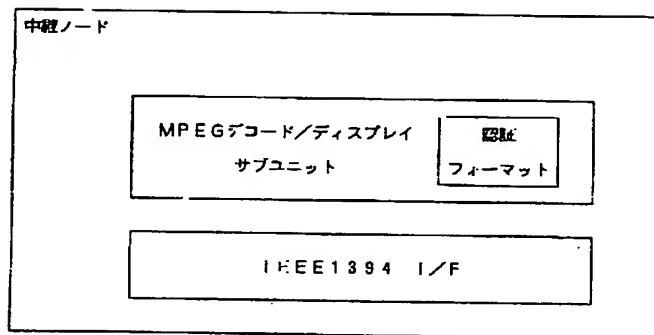
【図54】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード4101の映像送信サブユニット (認証フォーマット有)	映像送信サブユニット (認証フォーマット有)
送信ノード4101のパネルサブユニット	パネルサブユニット
⋮	⋮

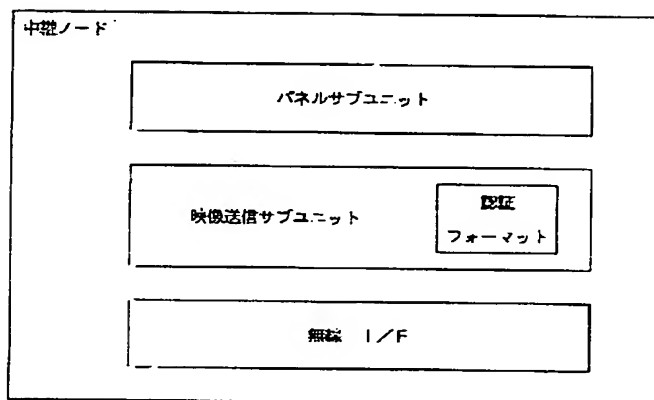
【図72】



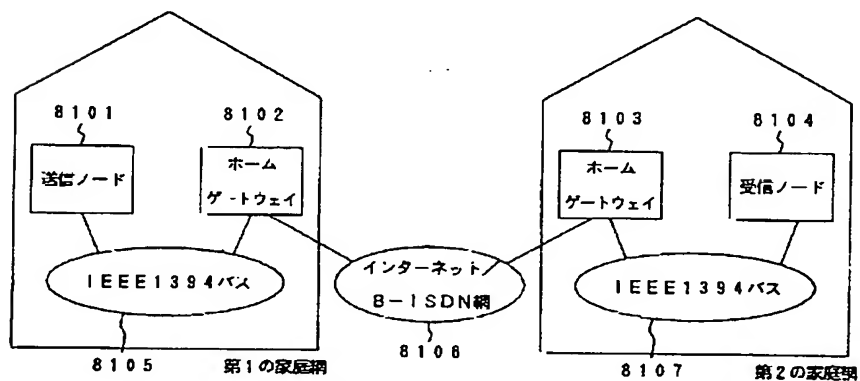
【図55】



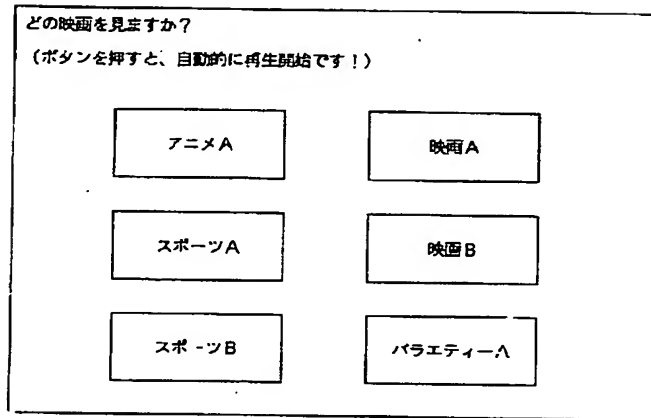
【図56】



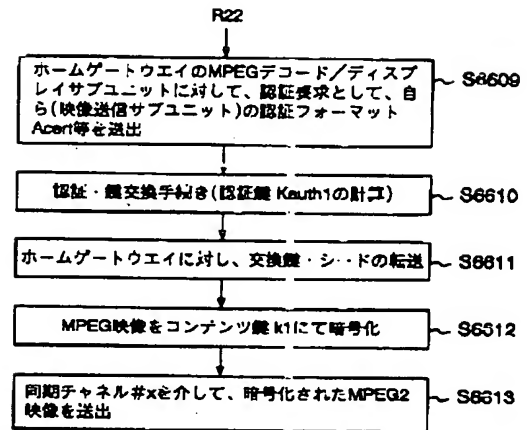
【図73】



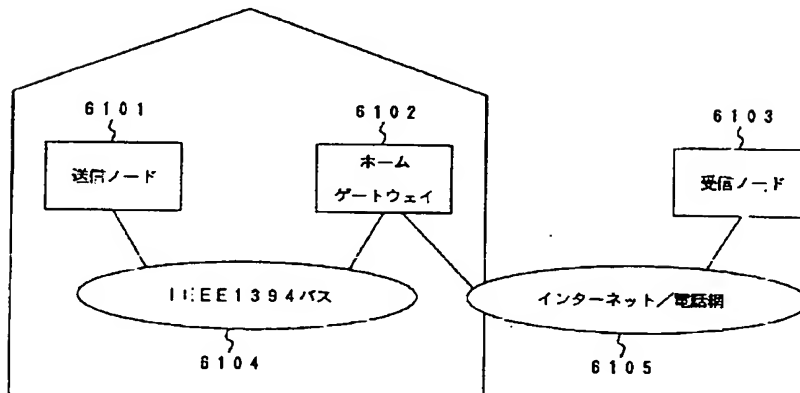
【図57】



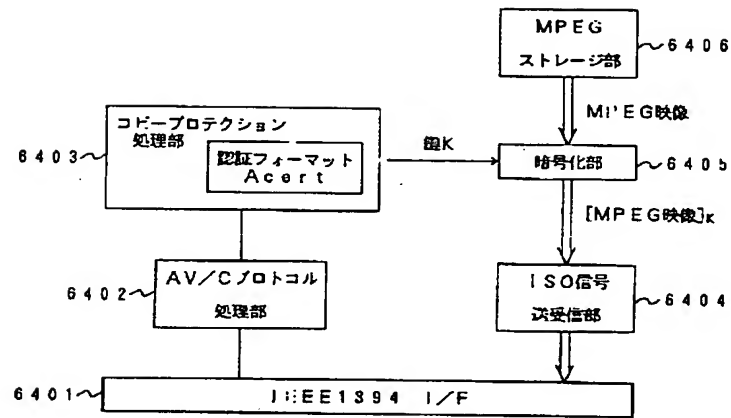
【図65】



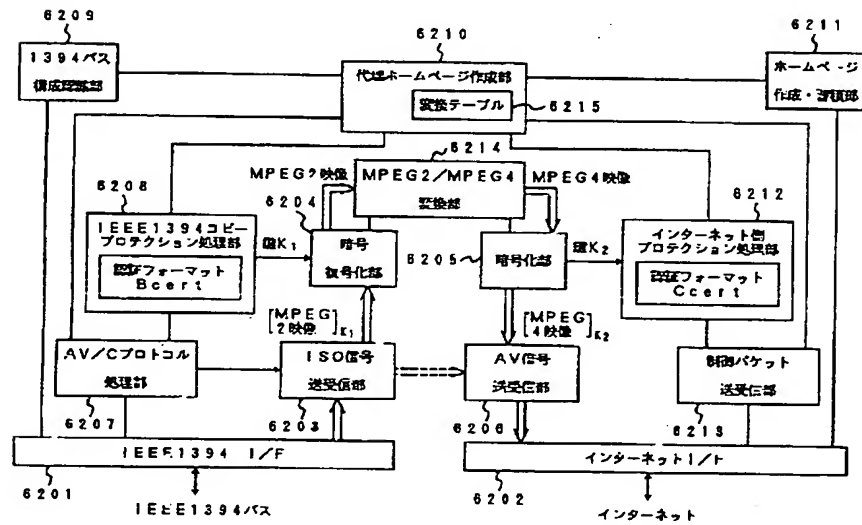
【図58】

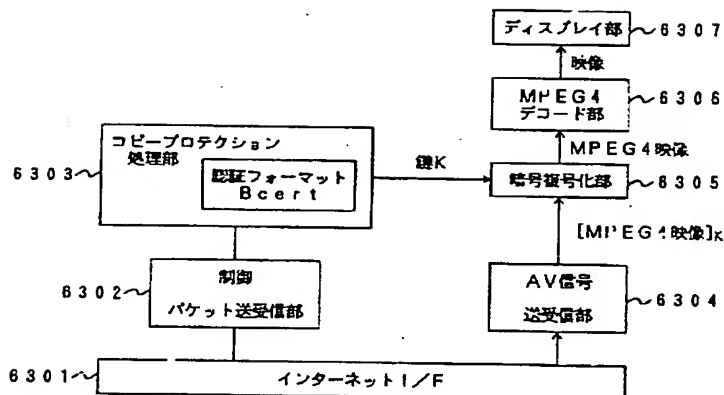


【図59】

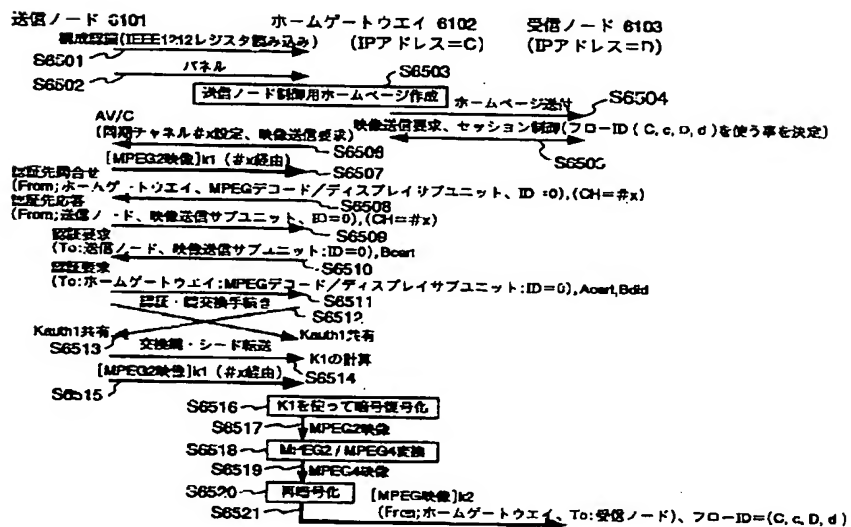


【図60】



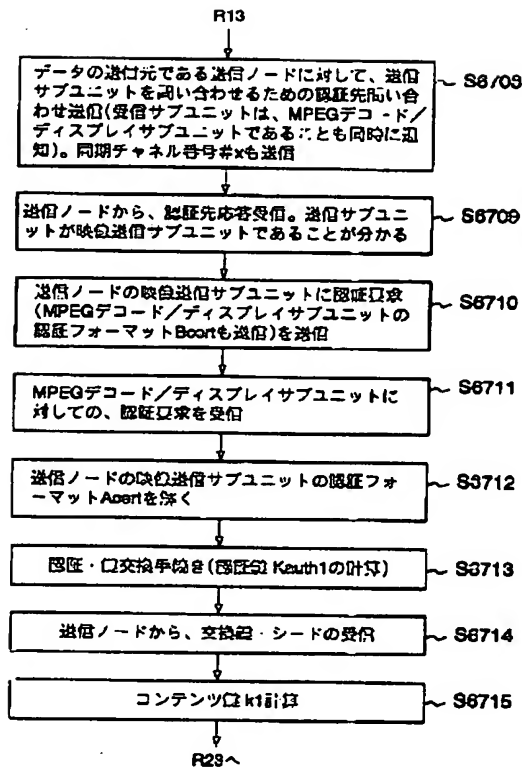


【图 6-2】

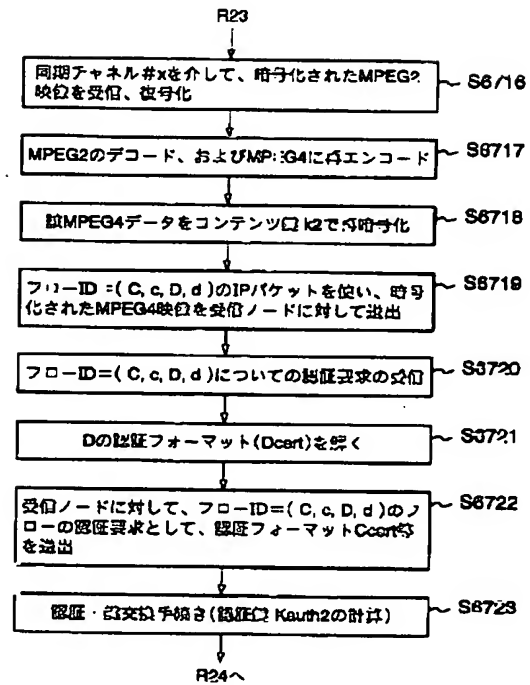




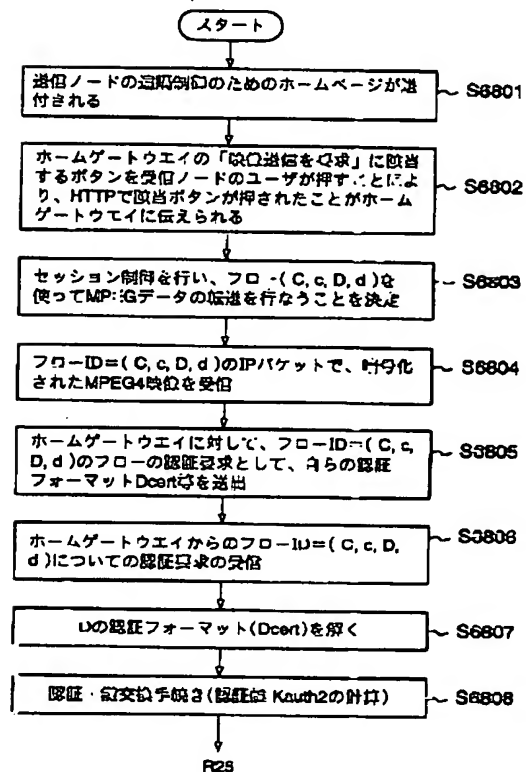
【図67】



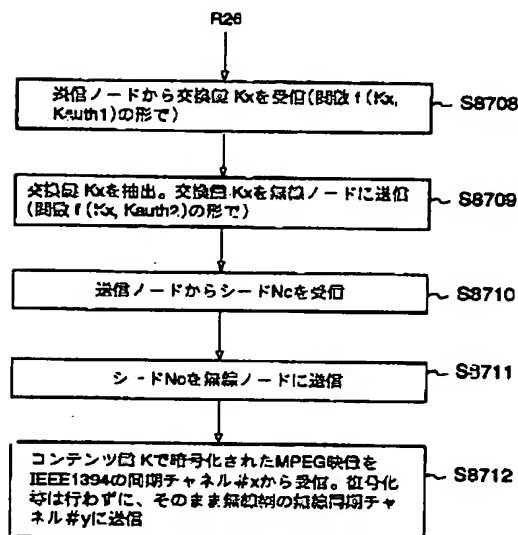
【図68】



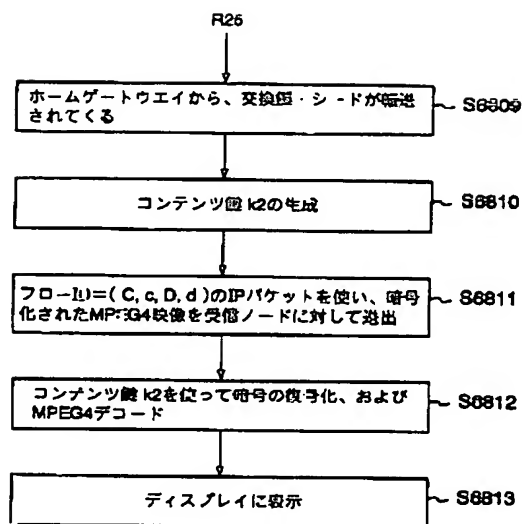
【図70】



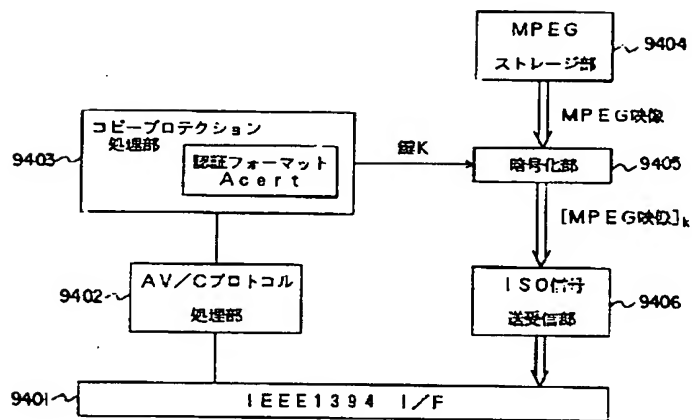
【図84】



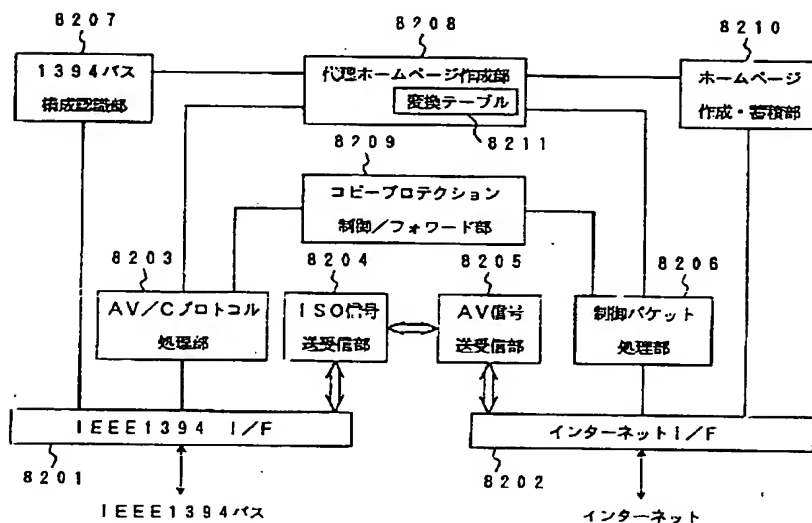
【図71】



【図78】

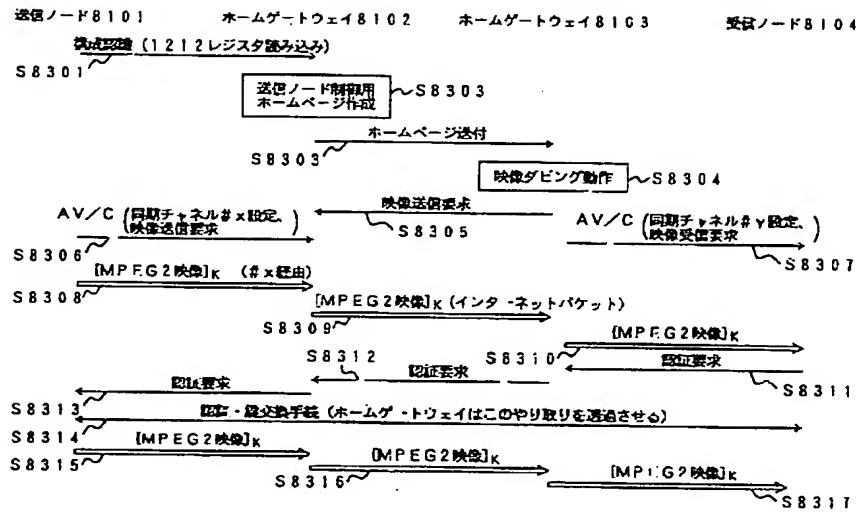


【図74】

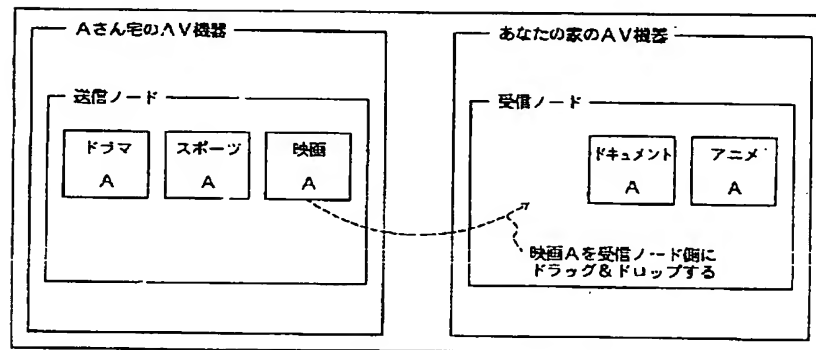




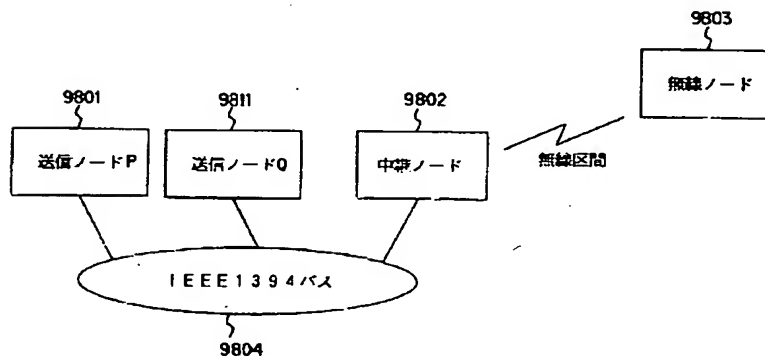
【図75】



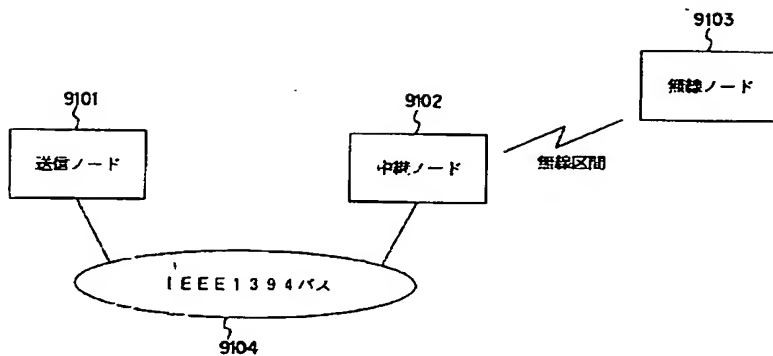
【図76】



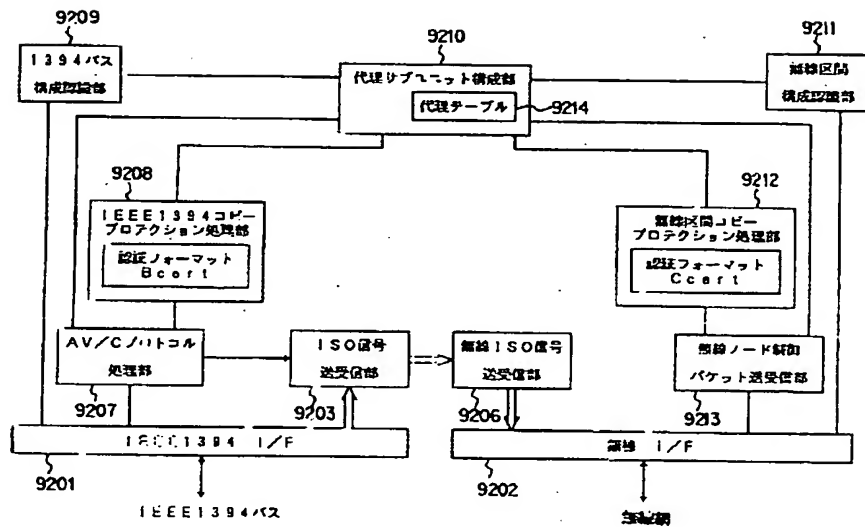
【図87】



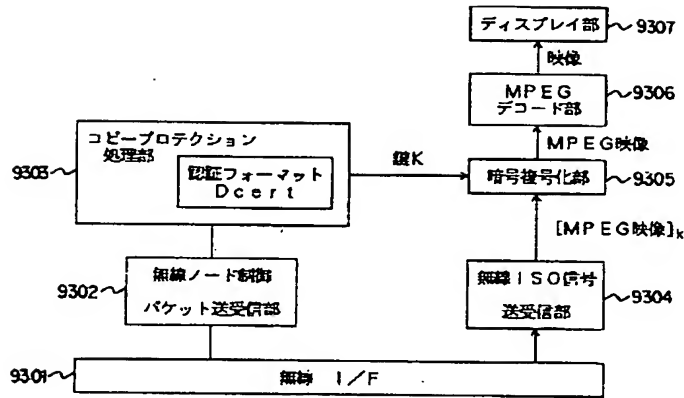
【図77】



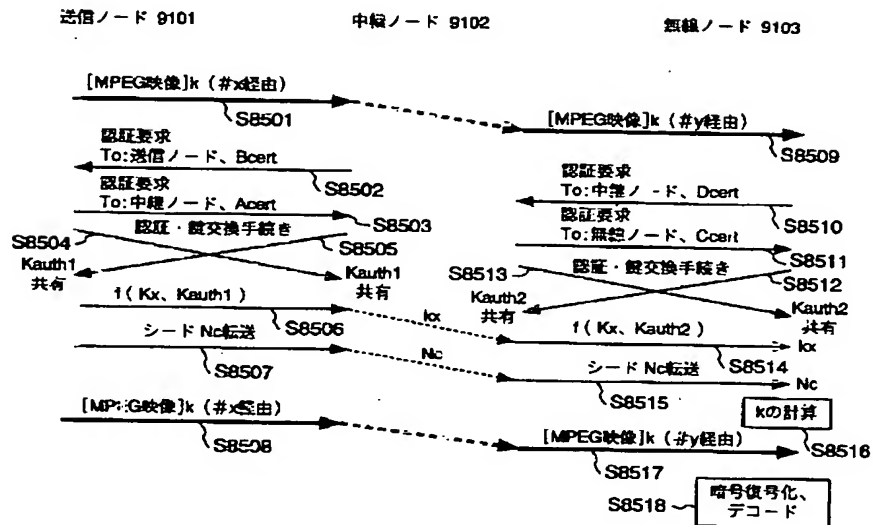
【図79】



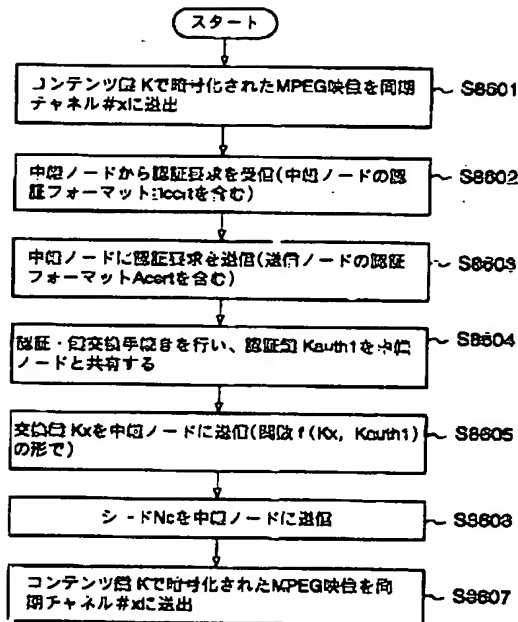
【図80】



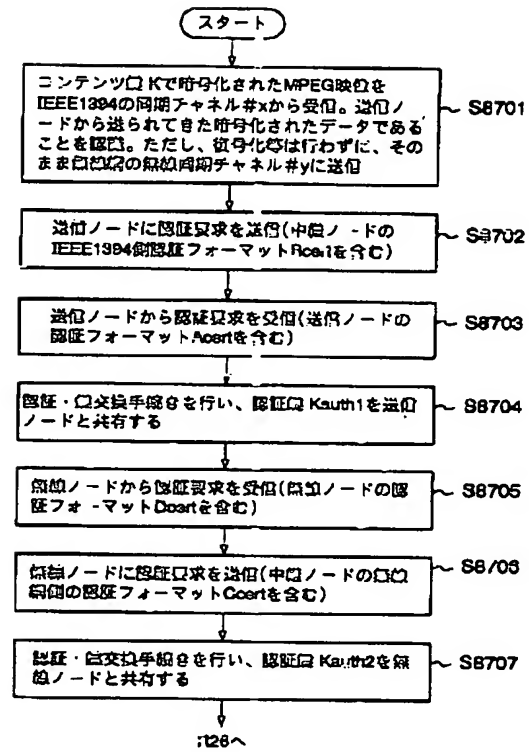
【図81】



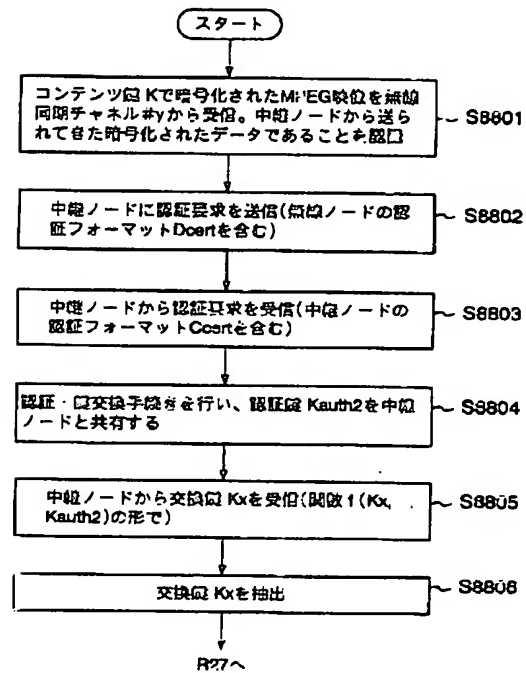
【図82】



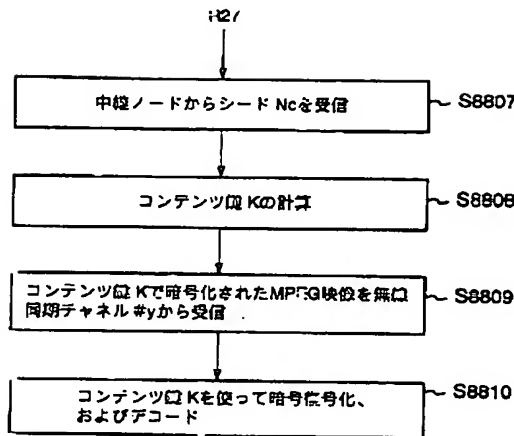
【図83】



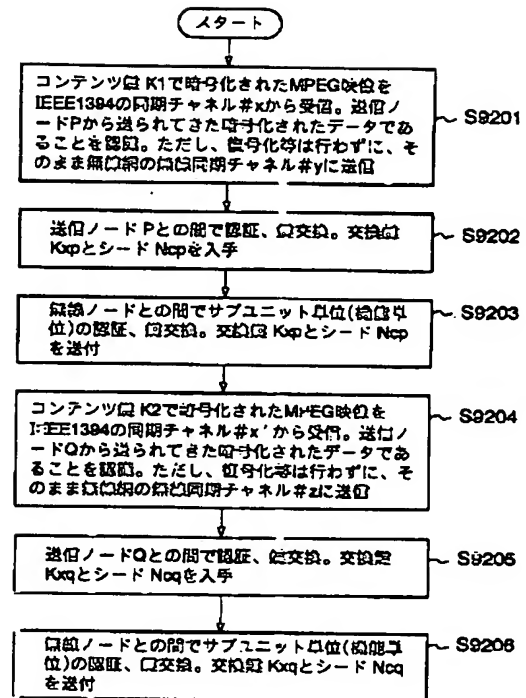
【図85】



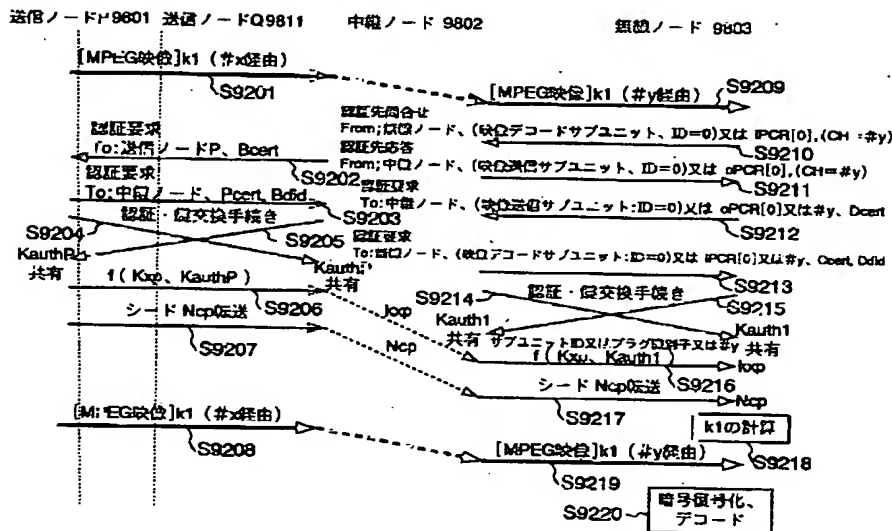
【図86】



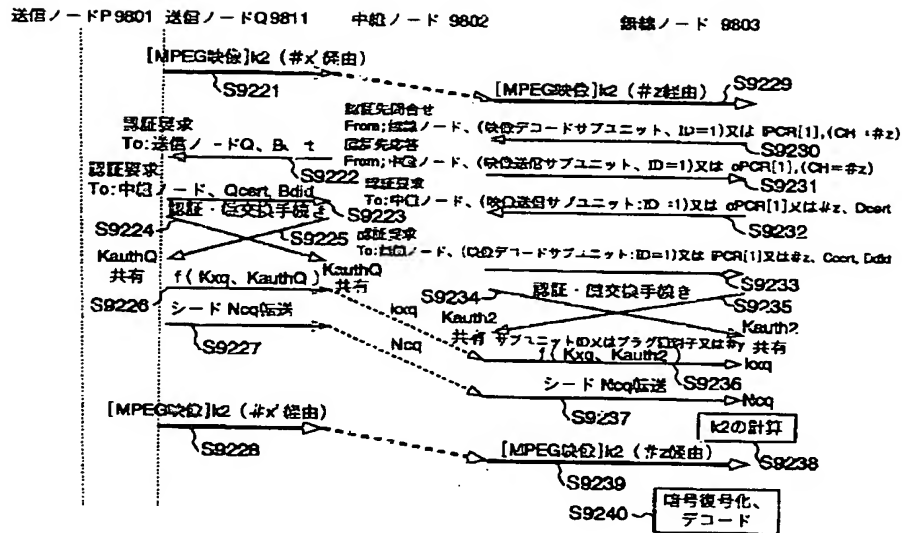
【図88】



【図89】



【図90】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

H 04 L 29/06

識別記号

F I

H 04 L 13/00

3 0 5 Z

(参考)

Reference No.:14002701

Delivery No.:002947

Delivery date: Heisei 18 January 6

---

NOTICE OF REASONS FOR REFUSAL

Patent application number	Patent application 2002-344431
Date of issue	Heisei 17 December 28
Patent office examiner	Junji Nakamoto 3140 5X00
Patent applicant attorney	Kenji Yoshitake (& 4 others)
Applied articles	Section 29 (2) and 36

This application is to be refused for the following reasons. If there are any arguments regarding this, please submit a statement of arguments within sixty days from a delivery date of this notice.

Reasons

[Reason 1 (inventive step)]

A patent shall not be granted for the invention related to the following claims of this patent application according to the provision of the Patent Law Section 29 (2) because the invention is an invention that could easily have been made, prior to the filing of the patent application, by a person with ordinary skill in the art to which the invention pertains, on the basis of an invention or inventions which were described in a distributed publication or made available to the public through electric telecommunication lines in Japan or elsewhere prior to the filing date of the patent application.

Note

(regarding cited documents etc., see the list of cited documents etc.)

- Claims 1, 3, 7, 8, 11-13
- Cited documents etc.,: 1-3

[Remarks]

(Regarding claims 1, 7, 12, 13)

There is shown that a communication device 10 (communication relay device) described in cited document 1 (refer to Paragraphs 13-42; Figures 1-6) transmits a homepage for authenticating users to a reproducer 20 when it accepts a request for a homepage for remote controlling from the reproducer 20, the reproducer 20 which received the homepage inputs a user ID and password (user authentication information) and transmits to the communication device 10, the communication device checks whether the received user ID and password are registered as a certified user in a database (authentication judgment means) and transmits a remote control homepage (a Web page describing information for controlling or monitoring the home communication device) to the reproducer 20 when the user ID and password are registered ones, the reproducer 20 transmits a request for a transmission of contents to a server 18 (home communication device) using the homepage for remote controlling, the server 18 transmits encrypted AV data to the communication device 10, the communication device 10 decrypts the encrypted AV data after performing an authentication / key exchange processing (first authentication and key exchange processing) by a first authentication / key exchange unit (first copyright protection unit) between the server 18, the communication device 10 then performs another encryption processing on the decrypted AV data and transmits to the reproducer 20, the communication device 10 performs an authentication / key exchange processing (second authentication and key exchange processing) between the reproducer 20 by a second authentication / key exchange unit (second copyright protection unit) when the communication device 10 transmits the encrypted AV data, and the reproducer 20 decrypts the received encrypted AV data.

Comparing an invention according to claims and an invention described in the cited document 1, they differ in the following points.

(1) On the communication relay device according to the claims,



authentication information of an outside communication device is registered and a transmission and reception of information is performed when the registration is confirmed, while on the communication device 10 described in the cited document 1, a registration of information of the reproducer 20 is not shown as a configuration and a transmission and reception of AV data is merely performed after a completion of user authenticating by the reproducer 20.

(2) In the invention according to the claims, a transmission and reception of information between the home network and outside network is performed when an authentication and key exchange by the first and second copyright protection means succeeds, while in the invention described in the cited document 1, the authentication and key exchange is performed after the transmission and reception of AV data.

However, (1) registering outside device information such as an access permission of an outside device is shown as outside device information 17c in cited document 2, paragraph 17. (2) Performing a transmission of encrypted AV data after a key exchange is also shown in cited document 3, paragraphs 53 and 54.

It is therefore admitted that a person with ordinary skill in the art can easily reach the invention according to the claims by applying methods described in cited documents 2 and 3 to the system described in the cited document 1.

(Regarding claim 3)

Using a device ID or physical address as identification data of outside device information is mere a matter determined appropriately by a person with ordinary skill in the art.

(Regarding claims 8, 11)

Setting a predetermined given value in a TTL field of a packet to be transmitted, utilizing a link local address, and using Ethernet (registered trademark) frame are admitted as a well-known art for a person with ordinary skill in the art, and

whether to perform a transmission and reception of packets using the well-known art is mere a matter appropriately accomplished by a person with ordinary skill in the art as necessary.

Performing such as encoding conversion at a relay device, protocol conversion, and bandwidth conversion is also a well-known art for a person with ordinary skill in the art.

[Reason 2 (improper description)]

This application does not satisfy the requirement under Patent Law Section 36(6)(i) for the following points.

#### Note

It is not clear where the statement in claim 4 "has a mode for storing a result of the second authentication and key exchange processing by the second copyright protection unit, in a state where an access to the home network is permitted to the outside communication device" is shown in the description of invention as an embodiment. Claim 4 is therefore not what described in the detailed description of invention.

No reasons for refusal are discovered at this time regarding an invention according to claims other than the claims objected in this NOTICE OF REASONS FOR REFUSAL. When any reasons for refusal are newly discovered, the reasons for refusal will be notified.

(In the statement "... the communication relay device according to claims 1 or 2" in claim 11, it is appeared to require a period at last (communication relay device\_.).)

#### List of cited documents etc.

1. Patent application laid-open 2001-285283
2. Patent application laid-open 2002-252882
3. Patent application laid-open 2002-140304

-----  
Record of prior art document search result



## 拒絶理由通知書

特許出願の番号	特願2002-344431
起案日	平成17年12月28日
特許庁審査官	中元 淳二 3140 5X00
特許出願人代理人	吉武 賢次 (外 4名) 様
適用条文	第29条第2項、第36条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から60日以内に意見書を提出して下さい。

## 理 由

## 【理由その1（進歩性）】

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第29条第2項の規定により特許を受けることができない。

記 (引用文献等については引用文献等一覧参照)

- ・請求項：1, 3, 7, 8, 11-13
- ・引用文献等：1-3

## [備考]

(請求項1, 7, 12, 13に対して)

引用文献1 (13-42段落及び図1-図6参照) 記載の通信装置10 (「通信中継装置」) は、再生装置20から遠隔制御用ホームページ要求を受け付けると、再生端末20に利用者認証用ホームページを送信し、それを受信した再生端末20では利用者ID及びパスワード (「ユーザ認証情報」) を入力して通信装置10に送信し、通信端末では受信した利用者ID及びパスワードが正規の利用者としてデータベースに登録されているか否かを照合し (「認証判定手段」)、登録されているものであれば遠隔制御用ホームページ (「宅内通信装置の制御または監視を行うための情報を記述したWebページ」) を再生端末20に送信し、再生端末20は遠隔制御用ホームページを用いてサーバ18 (「宅内通信装置」) にコンテンツ送信要求を行うと、サーバ18は暗号化AVデータを通信装置10へと送信し、通信装置10はサーバ18との間で第1の認証・鍵交換処理部

（「第1の著作権保護手段」）を用いて認証・鍵交換処理（「第1の認証鍵交換処理」）を行った後に当該暗号化AVデータを復号し、その後通信装置10は復号したAVデータを別の暗号化処理を施して再生端末20へと送信し、通信装置10は暗号化AVデータを送信すると、再生端末20との間で第2の認証・鍵交換処理部（「第2の著作権保護手段」）を用いて認証・鍵交換処理（「第2の認証鍵交換処理」）を行い、再生端末20では受信した暗号化AVデータを復号することが示されている。

そして、請求項に係る発明と引用文献1記載の発明とを対比すると下記の点で相違する。

（1）請求項に係る発明の通信中継装置では、宅外通信装置の識別情報を登録しておき、登録されていることが確認された場合に、情報の送受信を行っているのに対し、引用文献1記載の発明の通信装置10では、再生端末20の情報を登録しておくことは構成として示されておらず、単に再生端末20のユーザ認証完了後にAVデータの送受信を行っている。

（2）請求項に係る発明では、第1及び第2の著作権保護手段による認証鍵交換が成功した場合に、宅内ネットワーク及び宅外ネットワークの間の情報の送受信が行われているのに対し、引用文献1記載の発明では、AVデータの送受信が行われた後に認証鍵交換を行っている。

しかしながら、（1）中継装置に、宅外機器のアクセス許可等の宅外機器情報を登録しておくことは引用文献2の17段落に宅外機器情報17cとして示されている。また、（2）鍵交換を行った後に暗号化されたAVデータの伝送が行われることは引用文献3の53、54段落に示されている。

したがって、引用文献1記載のシステムに対し、引用文献2及び引用文献3記載の手法を適用し、請求項に係る発明とすることは当業者が容易に着想し得るものと認められる。

（請求項3に対して）

宅外機器情報の識別情報としてデバイスID又は物理アドレスを用いることは当業者が適宜決めればよい程度の事項である。

（請求項8，11に対して）

送信するパケットのTTLフィールドを予め決められた所定値を設定したり、リンクローカルアドレスを利用したり、イーサネット（登録商標）フレームを使用することは当業者にとって周知の技術であると認められ、それら周知の技術を用いてパケットの送受信を行うか否かは当業者が必要に応じて適宜なし得る事項である。

また、中継装置において符号化変換、プロトコル変換、帯域変換等の諸動作を行うことも当業者にとって既に知られている技術である。

【理由その2（記載不備）】

この出願は、特許請求の範囲の記載が下記の点で、特許法第36条第6項第1号に規定する要件を満たしていない。

## 記

請求項４に「前記宅外通信装置を前記宅内ネットワークに接続許可した状態で、前記第２の著作権保護手段による認証鍵交換処理を行った結果を登録するモードを持つ」とあるが、当該記載は実施例として発明の詳細な説明のいずれに示されたものであるのかよく分からず、したがって当該請求項４は発明の詳細な説明に記載されたものでない。

この拒絶理由通知書中で指摘した請求項以外の請求項に係る発明については、現時点では、拒絶の理由を発見しない。拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

（請求項 1 1 に「・・・請求項 1 または 2 に記載の通信中継装置」とあるが、最後に句点が必要である（「・・・通信中継装置。」）と思われる。）

## 引用文献等一覽

1. 特開 2001-285283 号公報
2. 特開 2002-252882 号公報
3. 特開 2002-140304 号公報

## 先行技術文献調査結果の記録

・調査した分野      I P C第7版    H04L12／28，46，56  
                               H04L9／32  
                               H04Q9／00

## DB名

・先行技術文献

1. 特開2000-174797号公報

(本願と出願人同一：中継ノードがコンテンツ保護を行うための手段を有する)

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。

この拒絶理由通知の内容に関するお問い合わせ

整理番号 14002701

発送番号 002947

発送日 平成18年 1月 6日 4/4

---

または面接のご希望がございましたら下記までご連絡下さい。

特許審査第四部デジタル通信 中元(なかもと)

TEL. (03) 3581-1101 内線 3594

FAX. (03) 3501-0699